AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES
J	1 | 66

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO.(If applicable)
0003	29-Dec-2004		

6. ISSUED BY	CODE	7. ADMINISTERED BY (If other than item 6)	CODE
NAVSEA INDIAN HEAD 101 STRAUSS AVE. ATTN: JESSICA D. MADDOX INDIAN HEAD MD 20640-5035	N00174	**See Item 6**	

8. NAME AND ADDRESS OF CONTRACTOR (No., Street, County, State and Zip Code)		
	X	9A. AMENDMENT OF SOLICITATION NO. N00174-05-R-0004
	X	9B. DATED (SEE ITEM 11) 04-Nov-2004
		10A. MOD. OF CONTRACT/ORDER NO.
		10B. DATED (SEE ITEM 13)
CODE	FACILITY CODE	

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

[X] The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offer [X] is extended, [ ] is not extended.

Offer must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended by one of the following methods: (a) By completing Items 8 and 15, and returning 1 copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

[ ] A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.

[ ] B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(B).

[ ] C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:

[ ] D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor [ ] is not, [ ] is required to sign this document and return _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of this amendment is to provide questions and answers concering the subject solicitation. Also provided is a revised Statement of Work and the Security Requirements Traceability Matrix. See page 2 for details.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) TEL: EMAIL:	
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA BY (Signature of Contracting Officer)	16C. DATE SIGNED 29-Dec-2004

SECTION SF 30 BLOCK 14 CONTINUATION PAGE

The following items are applicable to this modification:

CONTINUATION PAGE

1. The following questions and answers resulted from the site surveys conducted 13 through 15 December:

Question #1: Is there a particulate issue?
Answer #1: The racks installed at NAVEODTECHDIV do not need to be environmentally controlled. The racks installed at the gateway locations do need to be environmentally controlled.

Question #2: Have you modified the two spaces where the racks will be installed?
Answer #2: The modifications are underway.

Question #3: Do we have to provide power from the panel in to the room?
Answer #3: Depending on the UPS solution engineered, power can be provided either to the power distribution racks or just to the panel in the room. It is up to the offeror to clearly articulate power requirements as well as where they would like power to terminate (to include type of outlet and breaker on the circuit).

Answer #4: Will we have to provide UPS?
Question #4: Yes, protection for 45 minutes.

Answer #5: What level of power redundancy are you looking for?
Question #5: A/B within the farm. It is not the offeror's responsibility to deal with B side power to the room.

Answer #6: Do you want to see power proposed for ease of use?
Question #6: Yes.

Answer #7: Do you have floor plans that you can provide?
Question #7: Floors plans were provided with Amendment 0002. The diagrams are notional. Floor plans show where the AC units are installed.

Answer #8: Are the floor plans changed from the earlier market research survey?
Question #8: No.

Question #9: Do the floor plans reflect the HVAC ducting?
Answer #9: There is no ducting

Question #10: Is the plan that calls for the classified system in room 115, the unclassified system in room 119, and the development farm in room 115A firm?
Answer #10: Yes, however within each room it is the offeror's responsibility to develop the server farm floor plan within the room

Question #11: What does the RFP require for room 115A?
Answer #11: Only an extension of the cable management system.

Question #12: What kind of racks are in room 119?
Answer #12: The offeror is not responsible for any of the racks in RM 119

Question #13: How will disposal of the old racks be handled?
Answer #13: The Government will dispose of the old racks.

Question #14: Will the old racks be stored during migration?

Answer #14: Yes

Question #15: Do we have access to anything above the drop ceiling?
Answer #15: No.

Question #16: Based on the answer to the question above, what kind of cabling connections are required?
Answer #16: See the requirements for the cable management system

Question #17: What are you using to migrate the data? Do you want us to propose the easiest way to migrate the data? If there are things that we recommend, can we include them in the proposal?
Answer #17: Offerors are required to provide the information requested in the Instructions to Offerors. Offerors are also reminded that they will be evaluated in strict accordance with the information contained in Evaluation Factors for Award. Only that information requested in the Instructions to Offerors will be evaluated.

Question #18: Is it true that the Government will not allow patch cabling between the racks, only distribution cabling?
Answer #18: Yes.

Question #19: Are there requirements to seismically bolt the racks?
Answer #19: No.

Question #20: How do you want the racks set up?
Answer #20: It is up to the offeror to propose a solution that meets the requirements within the space provided.

Question #21: How will inspection occur prior to shipment?
Answer #21: It is up to the offeror to propose an inspection and acceptance plan.

Question #22: Is the majority of the data to be stored static, and if not, what percentage of the data is static?
Answer #22: Approximately 40% of the data is static.

Question #23: Will the Government provide anti-static flooring?
Answer #23: All flooring will be installed prior to installation of the server farms.

Question #24: Is there still a requirement for an additional 50% to account for power growth?
Answer #24: Yes.

Question #25: Where does the AB power come from and is that on the UPS as well? Will there be a transfer switch somewhere upstream? Does the Government want AB power delivered downstream of the UPS?
Answer #25: The offeror's only responsibility is to ensure AB power downstream of the UPS and account for the later addition of B side power upstream of the UPS.

Question #26: Originally, the Government requested different UPS units. Is this still the case?
Answer #26: The Government has never requested a specific UPS solution. It is up to the offeror to meet the terms of the SOW.

Question #27: How long will it be from proposal submission until contract award?
Answer #27: A conservative estimate is one month. Installation of the server farms will not begin until April 2005.

Question #28: Are we assuming responsibility for the switches?
Answer #28: See the revised SOW provided in Amendment 0002.

Question #29: What is the Government's minimum U requirement for each rack?
Answer #29: 42.

Question #30: What happened to the tape library? Is there still a requirement for a UPS for the tape library?
Answer #30: Tape library requirements have been removed. Please see the amended SOW.

Question #31: Is there still a requirement for environmentally controlled racks at the gateway sites?
Answer #31: Yes.

Question #32: Is this requirement connected to the InfoPro requirement?
Answer #32: No.

Question #33: When the new equipment is delivered, will it be set up with the existing equipment?
Answer #33: Partially until migration and then old equipment will be removed rack by rack.

Question #34: Will the power be three phase or single phase?
Answer #34: 3 phase.

Question #35: How high is the ceiling in room 119?
Answer #35: Please refer to the diagrams provided in Amendment 0002.

Question #36: Will there be a connection between rooms 115 and 119?
Answer #36: Fiber optic data cables will be the only connection between the rooms 115 and 119.

Question #37: Will the licensing be by user or by processor?
Answer #37: By processor.

Question #38: Can you provide a specific city for the gateway locations?
Answer #38: The gateways will be installed on large military installations in each of the countries specified.

Question #39: Can the spares kits be maintained at the depot?
Answer #39: No. Spares kits must be maintained at the sites where the racks are installed.

Question #40: Are you looking for multiple levels of defense in the intrusion detection system?
Answer #40: Offerors are responsible for engineering a solution and articulating that to the Government in their technical proposals.

Question #41: Is there a bandwidth requirement?
Answer #41: The gateway sites have T1 lines. The farms installed at NAVEODTECHDIV have 24 megabytes per second scalable to 6 DS3 lines.

Question #42: Is there an existing intrusion detection system?
Answer #42: No.

Question #43: Can the Government provide the number of users per gateway site?
Answer #43: No. The Joint EOD Community has 5,000 members on active duty, but the JEODNET supports more than the joint EOD community.

Question #44: Can the enterprise management system contain a SIM tool?
Answer #44: Yes, but it is the responsibility of the offeror to architect the solution and articulate that in their proposal

Question #45: Amendment 0002 provides two sets of requirements for Type 1 and 2 servers. The 1st set is on page 6 and 7 of the PDF document and differs from the 2nd set which is included in the amended SOW. Which requirements would the Government like us to respond to?
Answer #45: The requirements in the SOW are always the definitive requirements.

Question #46: The quality of the PDF version of the Gateway RP spreadsheet is extremely difficult to read. This vendor respectfully requests a readable copy.
Answer #46: As noted in the pre-solicitation notice, copies of all documents can only be obtained by downloading them from the Contracts Division's web site. Efforts will be made to make the Gateway RP spreadsheet more legible, but copies of the originals will not be provided via fax, mail, or e-mail.

Question #47: The NAS requirements provided on page 8 of the Amendment 0002 PDF document are not included as part of the SOW. Please advise if the Government intends to incorporate these into the amended SOW.
Answer #47: Refer to the storage requirements for the Gateways Section 4 of the SOW if a NAS is used these requirements apply

Question #48: In Section 3.2.4, Type 3 Server Requirements, the requirement that falls between numbers 75 and 76, Each server will contain a configured boot partition is not numbered. Please advise how we should reference that requirement or if the Government intends on renumbering the entire sequence following number 75.
Answer #48: Refer to the revised SOW found at the end of this amendment.

Question #49: There is no number assigned to the requirement stated in 3.6.2 Hardware, An empty (per server farm (total of 2)) rack that matches the other racks provided will be an additional CLIN.
Answer #49: There does not need to be a requirement number associated with providing an empty rack that matches the other provided.

Question #50: There are a number of references to Key Personnel Qualifications. Would the Government please provide this information?
Answer #50: Generating a staffing plan is the responsibility of the offeror. Qualifications of the individuals proposed and the mapping of qualifications to tasks are evaluation terms. Additionally, the qualifications of the personnel proposed will become the minimum personnel qualifications during the term of the contract. The Government considers all personnel proposed to be key.

Question #51: In Section 1.0 Scope, Phase 3 is referred to as Option 2 and Phase 4 as Option 3, but in Section 6, Phase 3 Tasks, Requirements and Deliverables, Phase 3 is referred to as Option 1 and in Section 7, Phase 4 Tasks, Requirements and Deliverables, Phase 4 is referred to as Option 2. Please clarify.
Answer #51: See amended SOW.

Question #52: Section 3.2.5 Special Requirements: Enterprise Distributed Backup System: The new requirement eliminates the requirement for a Backup Library Unit. The requirement states that the enterprise SAN at N1 must backup/replicate their file systems at the gateway (25% per gateway) as quickly as can be supported using half a T1 connection between N1 and the gateway. Is there a requirement for local backup, for example disk to disk at either the N1 and N2 sites? If there is such a requirement, will this be part of the 80 TB usable space or will it be an additional requirement?
Answer #52: All servers must backup to the SAN. The SAN will not replicate until off site solutions are online. This is part of the existing storage requirement, not a new requirement

Question #53: The Gateway locations are scheduled to be deployed in Phase 4 and this is an optional phase, what requirements for Backup will be in place prior to Phase 4?
Answer #53: Server to San -

Question #54: The Gateway locations are scheduled to be NAS devices of between 4 and 6 TB. The requirement for backup/replication calls for 25% per gateway. 25% of the 80 TB requirement is 20 TB.

This is between 3 and 5 times the NAS capability at the Gateway facility. Please reconcile this discrepancy or clarify.
Answer #54: See amended SOW.

Question #55: Section 3.2.5 Req. 107. The Enterprise SAN at N1. Calculating the bandwidth of ½ a T1 at 750kbs and ¼ of the SAN data at 20TB it will take several thousands of hours to replicate/backup the SAN data to the gateways sites. This offeror understands that the requirement is for "as quickly as can be supported," but also believes that this will provide NAVEOD an unworkable solution. Can the Government clarify that they understand the extended amount of time it will take to copy this data with the limited bandwidth provided or modify the requirements?
Answer #55: It is up to the offeror to articulate the issues and provide the best possible solution in their proposal.

Question #56: Section 3.2.5 Req. 105. All servers except those in the DMZ. For Servers 5 and 6 which have 1TB of local storage, does the Government intend to fully backup the 1TB of local storage to the SAN everyday? Due to the load imposed on the servers, local network and SAN by doing a full backup every day would the Government be willing to allow for incremental or differential backups to be done on a schedule with full backups done weekly or monthly?
Answer #56: No.

Question #57: Section 7.2.1 Req. 274. Each rack must contain Type 1 servers in conformance with section 3.1.2. There is no section 3.1.2. Does the Government intend for this requirement to read, "Each rack must contain Type 1 servers in conformance with section 3.2.2"
Answer #57: See amended SOW.

Question #58: Section 7.2.1 Req. 274. Each rack must contain Type 1 servers in conformance with section 3.1.2. It appears that the Government has removed the requirement for a SAN from this section but the requirement still exists for two Fiber Channel HBAs. Does the Government intend to add a requirement to Section 3.2.5 Special Requirements per Server by Number to remove the requirement for the HBAs as listed in the Type 1 Server section?
Answer #58: Section 7.2.1 refers to gateways storage can be either SAN or NAS. Pay attention to the volume requirements if the storage solution for the gateway sites is not FC SAN based then remove them from the GATEWAY solution. The Government will not alter type 1 requirements but will release the requirement for a GATEWAY if the offeror's proposal addresses enterprise storage access.

Question #59: Section 7.2.1 Req. 275. Each rack must contain Type 2 servers in conformance with section 3.1.3. There is no section 3.1.3. Does the Government intend for this requirement to read, "Each rack must contain Type 1 servers in conformance with section 3.2.3"
Answer #59: See amended SOW.

Question #60: Section 7.2.1 Req. 275. Each rack must contain Type 2 servers in conformance with section 3.1.3. It appears that the Government has removed the requirement for a SAN from this section but the requirement still exists for two Fiber Channel HBAs. Does the Government intend to add a requirement to Section 3.2.5 Special Requirements per Server by Number to remove the requirement for the HBAs as listed in the Type 2 Server section?
Answer #60: Section 7.2.1 refers to gateways storage can be either SAN or NAS. Pay attention to the volume requirements if the storage solution for the gateway sites is not FC SAN based then remove them from the GATEWAY solution. The Government will not alter type2 requirements but will release the requirement for a GATEWAY if offerors proposal addresses enterprise storage access.

Question #61: Section 7.2.1 Req. 281. NAS must connect using 100% redundant paths to the type 1 server cluster. It appears that the requirement for the Type 1 Server Cluster has been removed from the RFP, could the Government clarify where the requirement is for the Type 1 Server Cluster that the NAS device must have a connection to?
Answer #61: Redundant paths to the servers see amended SOW

Question #62: Section 7.2.1 Req. 281. NAS must connect using 100% redundant paths to the type 1 server cluster and type 2 server. A NAS device shares its storage via the Network, can the Government clarify if this is this a requirement for an additional network connection in addition to the already required 100baseT teamed NICs in this section?
Answer #62: See amended SOW

Question #63: Section 7.2.1 Req. 278. NAS can be either Fiber Channel or ATA and must... In addition to the ATA and Fiber Channel based NAS will the Government allow for a NAS device that is SCSI based?
Answer #63: Yes

Question #64: Section 7.2.1 Req. 267. Racks must comply with section 3.3. Section 3.3 is the SAN Storage Section. Can the Government clarify is this requirement is intended to reference Section 3.4?
Answer #64: See amended SOW.

Question #65: Section 7.2.1 Req. 267. Racks must comply with section 3.3. If this offeror proposes the Liebert rack model numbers provided in this solicitation can it be assumed that they will meet all the requirements as listed in Sections 3.4 and 7? If not, can the Government modify this requirement so that the Liebert rack model numbers specified will be acceptable?
Answer #65: The Govemment has reviewed and accepted the Leibert rack for gateway implementations due to the need to environmentally control the racks at a gateway location. General rack requirements will not be changed.

Question #66: In order for this vendor to properly respond to the technical requirements and fully comply contractually with the SOW, this vendor asks that the Government provide further clarification within the SOW reflecting any and all updates or changes to the requirements and discussions provided in Amendment 0002 as answers to questions.
Answer #66: It is up to the offeror to review the amended SOW for any and all changes. Many of the changes were identified in the questions and answers provided in Amendment 0002.

Question #67: Section 3.2.2 Type 1 Servers (Requirement 5). All drives will be the largest and fastest currently supported. Disk drives are available in several variants including two that are commonly configured into servers, SATA and SCSI. In both families of drives sizes and speeds do not necessarily correspond. For example in the SCSI disk drive family the 146GB disk drive is available in both the 10K RPM and 15K RPM variants whereas the 300 GB drive is only available in the 10K RPM variant. SATA drives have the comparable types of variations in speeds and sizes. Could the Government please clarify which drives they want to be configured into the Type 1 Servers.
Answer #67: It is the offeror's responsibility to engineer the solution based on the best solution for the intended purpose. The Government will not alter performance requirements or turn them into technical requirements that engineer the system for the offeror.

Question #68: Section 3.2.3 Type 2 Servers (Requirement 33). All drives will be the largest and fastest currently supported. Disk drives are available in several variants including two that are commonly configured into servers, SATA and SCSI. In both families of drives sizes and speeds do not necessarily correspond. For example in the SCSI disk drive family the 146GB disk drive is available in both 10K RPM and 15K RPM variants whereas the 300 GB drive is only available in the 10K RPM variant. SATA drives have the comparable types of variations in speeds and sizes. Could the Government please clarify which drives they want to be configured into the Type 2 Servers.
Answer #68: It is the offeror's responsibility to engineer the solution based on the best solution for the intended purpose. The Government will not alter performance requirements or turn them into technical requirements that engineer the system for the offeror.

Question #69: Section 3.2.4 Type 3 Servers (Requirement 62). All drives will be the largest and fastest currently supported. Disk drives are available in several variants including two that are commonly configured into servers, SATA and SCSI. In both families of drives sizes and speeds do not necessarily correspond. For example in the SCSI disk drive family the 146GB disk drive is available in both 10K RPM and 15K RPM variants whereas the 300 GB drive is only available in the 10K RPM variant. SATA drives

have the comparable types of variations in speeds and sizes. Could the Government please clarify which drives they want to be configured into the Type 1 Servers.
Answer #69: It is the offeror's responsibility to engineer the solution based on the best solution for the intended purpose. The Government will not alter performance requirements or turn them into technical requirements that engineer the system for the offeror.

Question #70: Section Diagrams. Rack 1 shows a Passport 8300 Perimeter Switch, Ext Firewall, VPN Gateway, Internal Firewall and a Passport 8600 Internal Switch. There is no mention in the SOW about this equipment. Could the Government clarify what if any the offeror's responsibility will be with regard to this equipment upon contract award.
Answer #70: This equipment is mentioned in the SOW and it is the offeror's responsibility to replace the equipment with the same or similar product

Question #71: Section Diagrams. Denotes hardware not covered by this procurement but must be factored in and supported by racks, power, and cabling covered under this procurement. Please clarify if this statement requires the offeror to provide a rack and supporting hardware for the equipment designated under the heading Rack 1.
Answer #71: No.

Question #72: Please clarify if all the equipment shown in the Rack 1 diagram is GFE and not covered under this procurement.
Answer #72: This equipment is covered under this procurement. Refer to the SOW. The diagrams were notional and merely reflect the existing farm.

Question #73: Section 7.2.1 Requirement 277. Each rack must contain 1 NAS with…JEODNET Gateway Rack Plan Rack 1 does not show a NAS. Please clarify whether or not Gateway Rack 1 does or does not require a NAS.
Answer #73: Refer to the amended SOW found at the end of this amendment.

Question #74: Section 7.2.1 Requirement 267 which incorporates by reference Section 3.3 Requirement 126. Each rack containing at least one server will contain 1 KVM unit. JEODNET Gateway Rack Plan Rack 1 does not show a KVM. Please clarify whether or not Gateway Rack 1 does or does not require a KVM.
Answer #74: All racks containing at least 1 server must include a KVM

Question #75: Section 7.2.1 Requirement 267 which incorporates by reference Section 3.3 Requirement 126. Each rack containing at least one server will contain 1 KVM unit. JEODNET Gateway Rack Plan Rack 2 does not show a KVN. Please clarify whether or not Gateway Rack 2 does or does not require a KVM. If Gateway Rack 2 does require a KVM per the Gateway Rack Plan Rack 2 diagram there is no rack space in which to put it. Please clarify what the Government requires for Keyboard/Mouse/Video access to the Gateway Rack 2 Servers.
Answer #75: All racks containing at least 1 server must include a KVM

Question #76: Section 7.2.1 Requirement. Prepended to the Statement of Work is a list of requirements labeled as NAS. These NAS requirements differ from those in the Statement of Work as listed in Section 7.2.1. With all due respect this offeror requests that the Government please clarify the requirements for the NAS device and incorporate them into Section 7.2.1 of the Statement of Work.
Answer #76: All requirements in the SOW are authoritative. The documents provided in Amendment 0002, other than the amended SOW, are provided for informational purposes only and do not alter the requirements contained in the RFP.

Question #77: Section 7.2.1 Requirement. Prepended to the Statement of Work is a list of requirements labeled as F5 3-DNS BOM. These requirements do not appear in the Statement of Work as listed in Section 7.2.1. With all due respect this offeror requests that the Government please clarify the requirements for the Gateway racks and devices and incorporate them into Section 7.2.1 of the Statement of Work.

Answer #77: There are only 2 items that have to be provided as already installed are the F53DNS and the Red Eagle gateways. The SOW reflects this and the BOM was provided to answer questions as to which make and model are required. The SOW has been updated to show the passport 8300, 8600 and DMZ switches must be replaced either 1 for 1 or with an equivalent device. The BOM was provided for outline to the offerors what an equivalent device would need to contain IRT a gateway implementation only.

Question #78: Answer to Question 25. The answer to this question provides a list of equipment formerly listed as not covered by this procurement. Please clarify where in the Statement of Work these items are listed. Also please clarify if this equipment is to be mounted into Rack 1 as shown in Diagram 1.
Answer #78: As they were formerly listed as not covered you will now find them listed as ancillary equipment under phase 1 of the SOW

Question #79: Section 6.2.2 - Can the Government clarify/answer the following: (a) What is the maximum bandwidth that passes through the Passport 8600 to NIPRNET (link size)? (b) Is there a redundant/failover link? (c) Is load balancing used on this link? (d) Is host intrusion detection (HIDS) on each of the servers required? (e) Is failover protection for Network Intrusion Detection (NID) required? (f) Are hot-spares or spare parts required for IDS hardware? (g) What type of system event and security logs must the IDS system be able to query, concatenate and analyze: firewalls, routers, servers?
Answer #79: (a) The passport 8600 has no direct connection to either the DMZ or directly to the NIPRNET. The passport 8300 has a 24mbps link to the DISA ATM backbone that is scalable up to 6 DS3 trunk lines. (b) There is a redundant/failover link. (c) Load balancing is used on this link. (d) The Government considers this type of decision to be engineering related as the Government does not know what system any offeror intends to propose and the specifications of said system the Government is not prepared to answer this question. It is the offeror's responsibility to engineer and propose the best system to meet the performance requirements in the SOW and CONOPS for JEODNET. (e) See answer to subpart D. (f) If hardware is part of your solution then the spare parts kit for the rack in which it is installed would need to include parts for the IDS. (g) All of the above (any item covered by this procurement).

Question #80: Section 7.2.1, Requirement 269. Each rack must contain 2 24 port 100baseI Nortel Bay Stack switches. The Gateway RP spreadsheet only shows a single 24 port Nortel Bay Stack switch in a single rack. Can the Government clarify if the spreadsheet or this requirement is correct and amend the incorrect requirement or diagram?
Answer #80: The gateway RP spreadsheet is not part of the SOW and is notional. It is intended to provide additional information to offerors, but it does not replace the requirements as set forth in the SOW. The SOW is authoritative.

Question #81: Section 7.2.1, Requirement 270. Each rack must contain 2 Nortel Alteon Firewall devices. The Gateway RP spreadsheet only shows a single Nortel Alteon Firewall device in a rack. Can the Government clarify if the spreadsheet or this requirement is correct and amend the incorrect requirement or diagram?
Answer #81: Please see the answer to question #81.

Question #82: Section 7.2.1, Requirement 272. Each rack must contain 2 (NSA certified) SafeNet Red Eagles. The Gateway RP spreadsheet only shows a single rack containing 2 SafeNet Red Eagle VPN devices. Can the Government clarify if the spreadsheet or this requirement is correct and amend the incorrect requirement or diagram?
Answer #82: Please see the answer to question #81.

Question #83: Section 6.2.1 and 6.2.2, Requirements 253 and 265. A requirement was added to the Enterprise Management System section and the Enterprise Intrusion Detection System section that reads as follows: System must be capable of audit log reduction. Please clarify.
Answer #83: Audit log reduction is a common industry term for a system that revues system and security audit logs and provides analysis and trend detection.

2. A revised Statement of Work can be found at the end of this amendment.

3. The JEODNET Security Requirements Traceability Matrix can be found at the end of this amendment. This matrix is provided for informational purposes only. The requirements called out in the Statement of Work are authoritative.

4. The tentative deadline for receipt of proposals is 3:00 PM on 18 January 2004. A subsequent amendment to the subject solicitation will be issued and will provide the definitive deadline for receipt of proposals.

5. The subsequent amendment will also provide revised Instructions to Offerors and Evaluation Factors for Award.

6. All other terms and conditions remain unchanged.

7. For additional information, contact Jessica Maddox at 301-744-6614.

Statement of Work
JEODNET Infrastructure Implementation

1.0 Scope

This statement of work (SOW) describes the contractor's tasks and materials required for the technical update of the Joint Explosive Ordnance Disposal Network's (JEODNET) enterprise controlling node (N1) and the initial roll out of 4 regional gateway nodes (N3.1-N3.4).

This contract uses a four phase approach, each phase is defined as;

- Phase 1 - Labor and materials for updating JEODNET's enterprise controlling node (N1) data center. This is a complete solution for building and maintaining 2 server farms 1 unclassified (NIPRNET) and 1 classified (SIPRNET) farm.

- Phase 2 – Support labor and materials for the migration of data, applications and services off of the existing server farms onto the new server farms procured under phase 1. Contractor will be required to work with the contractor/s currently providing systems administration support to JEODNET. Risk of successful data migration is not assumed by this contract.

- Phase 3 - (Option 1) Labor and materials to architect an implement an enterprise management system and enterprise intrusion detection system for JEODNET

- Phase 4 – (Option 2) Labor and materials for the initial roll out of JEODNET's first 4 OCONUS global gateway sites. Each gateway will consist of a NIPRNET and SIPRNET implementation. Gateways will be installed in Asia, Europe, Middle East, and Hawaii

This 4 stage approach has been outlined based on the logical progression of events required to successfully complete global implementation. Each Phase is comprised of specific timelines and dependencies leading into subsequent phases and have their own acceptance/evaluation criteria. Additionally each phase requires support labor categories that differ significantly.

All materials delivered must be newly manufactured no refurbished or repaired equipment can be delivered.

2.0 Background

The JEODNET is a tactical, mission critical information system that provides globally distributed information access/sharing, advanced security, and a completely web-service enabled user environment in scenarios where the accurate and timely delivery of tactical mission critical knowledge is crucial to the success of the mission. Compliant with DoD Architecture Framework, Joint Technical Architecture and the Global Information Grid (GIG) 2.0, JEODNET provides the Joint EOD community with a viable avenue to reach its interoperability and network centric warfare goals. JEODNET also houses the repository for the entire scope of EOD information.

Diagrams 4 and 5 have been provided as a general overview of JEODNET Conops.

3.0 Phase 1 Tasks, Requirements & Deliverables

3.1 Task - The contractor will deliver, install (on-site) and baseline configure materials as outlined by the following requirements. Requirements in this SOW are numbered and identified as either T for minimum technical or P for performance.

3.2 Materials & Requirements (Note 2 identical farms are to be built, 1 NIPRNET and 1 SIPRNET)

3.2.1 Server requirements – JEODNET employs servers that fall into 1 of 3 categories or "Types." Wherever a type of server is referred to in this or subsequent sections of this SOW the following requirements apply unless otherwise stated.

3.2.2 Type 1 Servers – Quantity 24 (12 per farm) shall meet the following minimum technical / performance specifications:

Requirements	#	
Servers will be no more than 2U (1 to 1.5 preferred)	1	T
Server will be loaded with Microsoft Windows 2003 Server Enterprise Edition unless otherwise specified under specific server requirements	2	T
Servers will be configured with a minimum of 4GB Ram unless otherwise specified	3	T
Servers will contain at least 4 hard drives	4	T
All hard drives will be the largest and fasteest currently supported unless otherwise specified under server specific requirements	5	P
Drive 1 will mirror drive 2	6	T
Drive 3 will be configured as a global hot spare	7	T
Drive 4 will be configured as a global hot spare	8	T
Each server will contain redundant, hot swappable power supplies	9	T
Each server will support remote management	10	P
Each server will accept shutdown commands from the power management and distribution system with adequate time to execute the shutdown process just prior to battery drain	11	P
Each Server will continuously report its health to the enterprise server management system	12	P
Each server will alert the enterprise server management system when its operational conditions fall outside the range of acceptable conditions	13	P
Each server will be imaged onto a separate hard drive partition from the partition on which the OS is loaded	14	T
Each server will be capable of and configured for possible clustering in the future	15	P
No optional or advanced services will be loaded with the operating system	16	T
Each server will be configured as a stand alone server unassociated with any domain (AD and other services will be installed later)	17	T
Each server will contain a configured boot partition	18	T
Each server will contain 2 Fiber GIG E NICs unless otherwise specified	19	T
Each Server will contain 1 serial port (2 preferred)	20	T
Each server will contain 2 USB ports	21	T
Each server will contain 2-32 bit processors	22	T
Each processor will be the fasted currently supported	23	P
Each server will contain a total 2 FC ports on separate cards at 2Gbps (2 ports on 1 card is acceptable but not preferred)	24	T
Each server will contain 1 DVD RW drive	25	T
Each server will contain 1 floppy drive	26	T
Each server will use a Hard Drive – CD – Floppy –PXE boot sequence that is interruptible	27	T
Each servers video card will support 1280 x 1024 resolution and 16.19 million colors	28	T

3.2.3 Type 2 Servers – Quantity 14 (7 per farm) shall meet the following minimum technical specifications:

Requirements	#	
Servers will be no more than 4U	29	T
Server will be loaded with Microsoft Windows 2003 Server Enterprise Edition unless otherwise specified under specific server requirements or Data Center Server Edition is required to support installed RAM	30	T
Servers will have a minimum of 8 GB RAM	31	T

Servers will contain at least 4 hard drives	32	T
All hard drives will be the largest and fastest capacity currently supported by the offeror at time of award	33	P
Drive 1 will mirror drive 2	34	T
Drive 3 will be configured as a global hot spare	35	T
Drive 4 will be configured as a global hot spare	36	T
Each server will contain 2 RAID controllers 1 active and cabled to all 4 drives a second inactive card that drives can be moved to should card 1 fail	37	T
Each server will contain redundant, hot swappable power supplies	38	T
Each server will support remote management	39	P
Each server will accept shutdown commands from the power management and distribution system with adequate time to execute the shutdown process just prior to battery drain	40	P
Each Server will continuously report its health to the enterprise server management system	41	P
Each server will alert the enterprise server management system when its operational conditions fall outside the range of acceptable conditions	42	P
Each server will be imaged onto a separate hard drive partition from the partition on which the OS is loaded	43	T
Each server will be capable of and configured for possible clustering in the future	44	P
No optional or advanced services will be loaded with the operating system	45	T
Each server will be configured as a stand alone server unassociated with any domain (AD and other services will be installed later)	46	T
Each server will contain a configured boot partition	47	T
Each server will contain 2 Fiber GIG E NICs unless otherwise specified	48	T
Each Server will contain at least 1 serial port (2 preferred)	49	T
Each server will contain 2 USB ports	50	T
Each server will contain 4 32 bit processors	51	T
Each processor will be the fastest currently supported	52	P
Each server will contain a total of 2 FC ports on separate cards (1 per card) at 2 Gbps	53	T
Each server will contain 1 DVD RW drive	54	T
Each server will contain 1 floppy drive	55	T
Each server will use a Hard Drive – CD – Floppy –PXE boot sequence that is interruptible	56	T
Each servers video card will support 1280 x 1024 resolution and 16.19 million colors	57	T

3.2.4 Type 3 Servers – Quantity 8 (8 processors per server) (4 per farm) shall meet the following minimum technical specifications:

Requirements	#	
Servers will be no more than 8U	58	T
Server will be loaded with Microsoft Windows 2003 enterprise Edition	59	T
Servers will have a minimum of 10 GB of RAM	60	T
Servers will contain at least 4 hard drives	61	T
All hard drives will be the largest and fastest capacity currently supported by the offeror at time of award	62	P
Drive 1 will mirror drive 2	63	T
Drive 3 will be configured as a global hot spare	64	T
Drive 4 will be configured as a global hot spare	65	T
Each server will contain 2 RAID controllers 1 active and cabled to all 4 drives a second inactive card that drives can be moved to should card 1 fail	66	T
Each server will contain redundant, hot swappable power supplies	67	T
Each server will support remote management	68	P
Each server will accept shutdown commands from the power management and distribution system with adequate time to execute the shutdown process just prior to battery drain	69	P
Each Server will continuously report its health to the enterprise server management system	70	P

Each server will alert the enterprise server management system when its operational conditions fall outside the range of acceptable conditions	71	P
Each server will be imaged onto a separate hard drive partition from the partition on which the OS is loaded	72	T
Each server will be capable of 4 way clustering	73	P
No optional or advanced services will be loaded with the operating system	74	T
Each server will be configured as a stand alone server unassociated with any domain (AD and other services will be insttalled later)	75	T
Each server will contain a configured boot partition	B1	T
Each server will contain 2 Fiber GIG E NICs unless otherwise specified	76	T
Each Server will contain 1 serial port (2 preferred)	77	T
Each server will contain 2 USB ports	78	T
Each server will contain 8 32 bit processors	79	T
Each processor will be the fastest currently supported	80	P
The Cluster of 4 servers per farm will support Oracle 9i enterprise edition	81	P
Each server will contain a total of 2 FC ports on separate cards at 2Gbps	82	T
Each server will contain 1 DVD RW drive	83	T
Each server will contain 1 floppy drive	84	T
Each server will use a Hard Drive – CD – Floppy –PXE boot sequence that is interruptible	85	T
Each servers video card will support 1280 x 1024 resolution and 16.19 million colors	86	T

3.2.5 Special Requirements per Server by Number – Please refer to Diagram 1 to map servers to server number and rack. (Note Diagram 1 is not an authoritative, proposed or binding racking plan and is provided for clarity only) General minimum technical/performance requirements per server type apply unless superceded by these requirements.

Rack	Server Number	Requirement	#	
3	3 & 4	Each will have redundant 100baseT NICs teamed & connected to the DMZ switch	87	T
	5 & 6	Each will have redundant 10/100/1000baseT NICs teamed & connected to the DMZ switch	88	T
		Each will support 1 TB internal physical storage in a separate raid controller than the 4 drives supporting the OS	89	T
		Each will be loaded with Windows Server 2003 Web Server Edition	90	T
4	7&8	Each will be configured with 2 10/100/1000BaseT NICs teamed and connected to the Passport 8600 Internal switch	91	T
		Each will be configured with 2 FC Cards with 1 connection to each of the FC switches in the SAN	92	T
	9 & 10	Each will be clustered (clustering will be configured as part phase 2)	93	P
		Each will be configured with 2 1000baseF NICs teamed and connected to the Passport 8600 Internal Switch	94	T
		Each will contain 2 FC Cards with 1 connection to each of the SAN switches	95	T
6	Server Farm Printer	Will be a high-end color laser printer network attached to the Passport 8600 Internal switch using a 100BaseT connection	96	T
	11&12	Each will contain 2 1000BaseF NICs, but only 1 will be connected to the Passport 8600 Internal switch	97	T
7	13,14 & 15	Will be loaded with Windows Server 2003 standard edition and do not need to be able to support clustering	98	T
		Each will contain 2 10/100/1000BaseT NICs teamed and connected to the Passport 8600 Internal switch	99	T

		Each will contain 1 FC card 2 will be routed to SAN switch 1 and 1 will be routed to SAN switch 2	100	T
	16&17	Each will contain 2 1000BaseF NICs but only 1 will be connected to the Passport 8600 Internal switch	101	T
9	18,19, 20 & 21	Will be 4 way clustered (clustering will be configured as part of phase 2)	102	T
		Each will contain 2 1000BaseF NICS teamed and connected to the Passport 8600 Internal Switch	103	T
		Each will contain 2 FC Cards with 1 connected to SAN FC switch 1 and 1 connected to SAN FC switch 2	104	T
	Enterprise Distributed Backup System (1 per farm)	All servers except those in the DMZ must connect to the SAN or NAS and be able to fully backup all local storage to the SAN or NAS File System once per day and the process per server can not take longer than 1 hour per 100GB of local storage	105	P
		The Enterprise SANs at N1 (NAVEODTECHDIV) must be able to support full replication to an identical SAN at NAVSCOLEOD (N2) as quickly as can be supported using 5MBPS of bandwidth between N1 and N2 Note: this must be supported but implementation will be part of a follow on contract	106	P
		The enterprise SAN at N1 must backup/replicate their file systems to the NAS file system at the gateway (25% per gateway) as quickly as can be supported using half a T1 connection between N1 and the gateway Note: this is a distributed backup solution	107	P
		Backup solution must support being both file based and snapshot drive based (Servers need only support file based backup)	108	P
		Where file based backup occurs the backup of open files must be supported	109	P
		Enterprise backup solution must subscribe to the enterprise management solution	110	P
		An enterprise backup test plan must be supplied as part of the proposal	111	
		A server farm backup plan mu st be provided with the proposal	112	

Additionally the following ancillary equipment must be provided:

I. Nortel Passport 8300 Series perimeter switch or equivalent (also to be used in phase 4 gateways) QTY 2 (1 NIPR and 1 SIPR)

Current Implementation	Nortel Passport 8603 3-slot Chassis Bundle. Includes 8003 chassis, one 3-slot AC power supply, one 8691SF Switch Fabric and Routing Software License. (Includes North American power cord). (DS1412E06)
	8616GTE Routing Switch Module - 16 port 1000BASE-T Gigabit Ethernet interface module. (DS1404034)
	8648TXE Routing Switch Module. 48 port autosensing 10BASE-T/100BASE-TX Ethernet Layer 3 Switching interface. (DS1404035)

II. Nortel Passport 8600 Series backbone switch or equivalent QTY as many as are required to cover all equipment under this procurement in addition to supporting their current level of saturation

III. L3 Red Eagle VPN gateways (also to be used in phase 4 gateways) QTY 4 (2 NIPR and 2 SIPR)

IV. Nortel Alteon Firewalls or equivalent (also to be used in phase 4 gateways) QTY 4 (2 NIPR and 2 SIPR)

Current Implementation	Alteon Firewall 5106 - Non-accelerated ASF with 4x 10/100 Ethernet copper ports. (EB1639107)
	Check Point Enterprise-U-NG (CPVP-VCT-U-NG)
	VPN-1 Pro Gateway (CPMP-VPG-U-NG)

V. Nortel Baystack DMZ Switch or equivalent (also to be used in phase 4 gateways) QTY 2 (1 NIPR and 1 SIPR)

Current Implementation	BayStack 470-24T Switch - 24 10/100BASE-TX ports plus 2 built-in GBIC slots and built-in stacking ports. 18 in. stacking cable included. (Includes North American power cord) (AL2012E37)

3.3 Storage Requirements

3.3.1 Storage Area Network (SAN) – Quantity 2 (1 per farm) A new SAN shall be implemented that meets the following requirements.

Requirements	#	
SAN shall be 80 Terabytes in usable capacity and support Raid 5	113	T
SAN architecture must be scalable to 1000 Terabytes physical capacity and support Raid 5	114	T
All Firmware, software and components must have the most current update	115	T
SAN must contain at least 2 FC Switches	116	T
SAN must be configured to provide 100% redundant FC paths	117	P
SAN must contain 100% redundant controllers	118	P
SAN must contain 100% redundant cache of the largest size currently supported	119	P
SAN components must contain 100% redundant hot swappable power supplies with adequate UPS	120	P
SAN must be monitored by the Enterprise Management System	121	P
SAN must support the primary and redundant connection of at least 24 servers (switching and cabling must be included with the network maps and cabling plan)	122	P
SAN must be 100% Fiber Channel at the fastest speed supported	123	P
Must be an all new solution to include 100% redundant paths and all SAN hardware must have as much redundancy built in as can be currently supported (i.e. controllers, switches, power supplies, cache) . Existing SAN cannot be leveraged as part of this solution	124	P

3.4 Rack Requirements – All racks shall meet the following minimum technical specifications:

Requirements	#	
Each rack containing at least 1 server will contain 1 KVM unit	125	T
Each KVM unit will support all of the servers in that rack	126	P
Each KVM unit will support keyboard based switching between servers	127	T
Each KVM unit will contain a 17" flat panel TFT display that supports 1280 x 1024 resolution and 16.19 million colors	128	T
Each KVM unit will be no more than 1 U	129	T
Each KVM unit will use a miniature trackball, not track pad or stick mouse	130	T
Each Trackball will support the 2 button (right and left click) configuration	131	P
All racks will be the same color	132	P
All racks will be either opal (off white) grey, navy blue, graphite, or black	133	P
All components in the rack will be the same color as the rack	134	P
All open space in the front of the rack will be covered using metal spacers	135	P
The front door of the rack will be lockable and TRANSPARENT or grated allowing at least 60% visibility (tinted Plexiglas or glass is acceptable)	136	P
Any side doors to the rack will be lockable	137	P
The sides of all racks will be closed	138	P
The back of the rack will be closed but allow for adequate ventilation	139	P
Each rack will contain adequate active or passive ventilation for the equipment contained therein (Racks do NOT need to be environmental filtered)	140	P
Each rack will contain an internal cable management system	141	P
All servers will be rail mounted	142	P
All servers will have cable guides that will support the exposure of the server on its rails	143	P
All racks will support access to all hardware elements without the components being physically removed from the rack	144	P
All racks will be the same height and depth	145	P
All racks will support 28" FUNCTIONAL SERVER depth	146	T
All racks will support at least 42U of Height	147	T
Each rack will contain an internal power distribution system that plugs into an upstream power distribution rack and will support 30% power capacity expansion	148	P
All KVM switches in the rack will be connected to an upstream KVM unit for the entire farm where switching will be based on rack then server	149	P
Each Server farm will contain a 60" plasma display fed by the upstream KVM unit that supports at a minimum 1280 x 1024 resolution and 16.19 Million colors	150	P
Each server farm will contain a keyboard and mouse fed by the upstream KVM unit	151	P
Each rack will contain at least 6U of empty expansion space	152	P

3.5 Spare Parts Kit Requirements – The following denotes required spare parts kits and the requirements for these kits;

Requirements	#	
Every server will have 1 spare parts kit	153	P
Each kit will enclosed in a semi rugged, transportable case	154	P
Each kit will be labeled by rack and parent server	155	P
Each kit will protect all contents using foam matting	156	P
Each part will be enclosed in an anti-static bag	157	P
Each kit will include a spare power supply	158	P
Each kit will include 2 spare RAM chips	159	P
Each kit will include 1 spare hard drive	160	P
Each kit will include 1 spare RAID controller (unless controllers for the server are embedded on the mother board)	161	P
Each kit for a server containing FC cards will include 1 spare FC card	162	P

Each kit for a server containing a Fiber GIG E NIC will include 1 spare NIC	163	P
Each kit for a server containing a Copper GIG E NIC will include 1 spare NIC	164	P
Each kit will include any other items deemed appropriate by industry best practice or items known to have over a 75% failure rate	165	P
Each kit will include an anti-static grounding strap	166	P
Each kit will include any special tools required for server access and or part replacement	167	P
Each kit will contain a bound paper copy of all technical documentation for the server and all additional parts therein.	168	P
Each kit will contain a spare parts list for the associated server and contact information for obtaining these parts directly from the manufacturer	169	P
Each kit will contain an electronic copy of all technical documentation on CD or DVD for the server and all additional parts therein in a format approved by the COR	170	P
Each kit will contain a copy of the applicable warranty information for the server and all additional parts therein	171	P
Each kit will contain a copy of the applicable enterprise service agreement information for the server and all additional parts therein	172	P
Every rack will have 1 spare parts kit (for rack and racking equipment only)	173	P
Each kit will be labeled by rack number	174	P
Each Kit will contain a spare KVM switch	175	P
Each kit will contain a spare KVM switch to server cable	176	P
Each kit will contain a spare KVM switch to KVM unit cable	177	P
Each kit will protect all contents using foam matting	178	P
Each kit will include any other items deemed appropriate by industry best practice	179	P
Each kit will include an anti-static grounding strap	180	P
Each kit will include any special tools required for rack access and or part replacement	181	P
Each kit will contain a bound paper copy of all technical documentation for the Rack and all additional racking components therein.	182	P
Each kit will contain a spare parts list for the rack and contact information for obtaining these parts directly from the manufacturer	183	P
Each kit will contain an electronic copy of all technical documentation on CD for the rack and all additional racking components therein	184	P
Each kit will contain a copy of the applicable warranty information for the rack and all additional racking components therein	185	P
Each kit will contain a copy of the applicable service agreement information for the rack and all additional racking components therein	186	P

3.6 Physical Installation Requirements

3.6.1 Racks –

Requirements	#	
NIPRNET Server farm racks will be physically installed and cabled at NAVEODTECHDIV Building 2172 in Room 119 as per an approved racking plan	187	P
SIPRNET Server farm racks will be physically installed and cabled at NAVEODTECHDIV Building 2172 in Room 115 as per an approved racking plan	188	P

3.6.2 Hardware -

An empty (per server farm (total of 2)) rack that matches the other racks provided will be an additional CLIN.

3.6.3 Power – power management and distribution racks

Requirements	#	
Each farm will contain power management and distribution racks	189	P

Racks will conform to the requirements set forth in the rack section	190	P
Requirement removed due to replacement of Backup library with EDBS	191	P
The SAN must have its own free standing UPS unit or subscribe to a farm UPS system	192	P
All power distribution racks will provide power conditioning, filtering and surge suppression	193	P
Each rack will provide 45 minutes of battery power for the equipment in all connected downstream racks	194	P
Racks will be engineered to the power requirements of the racks they support with room for 30% capacity expansion	195	P
Due to the possible weight of these racks once configured, they may be configured ON-SITE at NAVEODTECHDIV; however, their design and specs must be pre-approved and on-site testing will determine acceptance	196	P
If configured on-site all components must be delivered as per the requirements under the deliverables section	197	P
Power distribution racks need to support A/B power from the distribution rack to all rack equipment	198	P
Each power distribution rack will support no more than 2 downstream equipment racks	199	P

3.6.4 Cable Management & Labeling

Requirements	#	
Inter-rack cable management system must be free standing and conform to Diagram 3	200	P
Inter-rack cable management system must route data cables high	201	P
Inter-rack cable management system must route power cables low or if routed high must electromagnetically insulate power and data from each other	202	P
Inter-rack cable management system cannot be bracketed to the wall or ceiling	203	P
Inter-rack cable management system must run between and above all racks as per Diagram 3	204	P
Inter-rack cable management system must be open mesh basket conduit based to support the free breakout of cables from the management system to the internal rack management system	205	P
All cables supporting the equipment under this procurement must be properly labeled on each end just prior to the connector and must denote source and destination rack, equipment number and port number (to include patch panel and port number)	206	P
All equipment must be labeled by number on the front and back	207	P
All racks must be labeled by number on the front and back by using an engraved metal plate label	208	P
All equipment ports must be labeled by number	209	P
All cables between racks will run from equipment to patch panel in the same rack; then patch panel to a patch panel in the destination rack then to destination equipment	210	P
All inter-rack cabling will be shielded and plenum based	211	P
All fiber cables between racks will be 4 strand multi-mode fiber (2 strands active and 2 spare)	212	P
2 strand (Zip cord) will only be used internally to the rack between equipment or equipment to patch panel in the same rack	213	P
All fiber patch panels will use ST or SC connectors or to miniaturize and save space MT-RJ connectors are acceptable but cost must be justified	214	P
All data cabling between racks in the NIPRNET Farm will be GREEN	215	P
All data cabling between racks in the SIPRNET Farm will be RED	216	P

3.7 Technical Support Requirements

Requirements	#	
The contractor will pre-register, and where applicable, activate all delivered hardware and software components before delivery, and associate all components with a site technical support agreement	217	P
For software requiring activation or registration that is either not preinstalled or preconfigured, the vendor will deliver the activation codes with the component (the customer will not be	218	P

burdened with registration or activation of any component)		
All components will be registered to FIRST NAME= JEODNET LASTNAME= CIO ADDRESS= 2008 Stump Neck Rd, Indian Head, MD 20640 PHONENUMBER= 301-744-4061 EMAIL= Trouble.Call.Desk@JEODNET.mil. No other information can be provided during the registration process without specific prior approval from the COTR	219	P
All delivered components will fall under a 5 year on-site enterprise service agreement for JEODNET	220	P
The onsite address for the components under this phase for the service agreement will be NAVEODTECHDIV 2008 Stump Neck Rd, Indian Head, MD 20640, 301-744-4061	221	P
The Enterprise service agreement will have a 4 hour maximum on-site response time from the point of initial contact between JEODNET and the service organization	222	P
The Enterprise service agreement will specify overnight same day shipping for repair and replacement parts BEFORE the return of the defective or broken part	223	P
Warranty coverage for all components will be extended to a 5 years	224	P
Warranty coverage will begin upon initial acceptance of ALL components (material CLINs) under this phase of procurement (Note – final acceptance will not occur until phase 2)	225	P
Service Agreement Coverage will begin upon delivery of components to NAVEODTECHDIV as per the delivery requirements	226	P

4.0 Deliverables

Deliverable	Scheduled Delivery Date
Material racks prefabricated with all equipment as per the approved racking plan and sections 4.2 and 4.3 of this SOW	45 calendar days from receipt of purchase order for the CLIN representing that rack
Applicable Software/Hardware Licenses and activation codes organized and delivered with original installation media (and a master listing of all installation and activation codes) as a package	End of phase 1 (10 working days from the delivery of all racks procured by CLIN under this phase), a working copy of installation media with installation /activation codes will be delivered with the rack containing the equipment upon which the software/component is installed
Template for delivery of final support documentation for approval	30 calendar days from contract award
Final Support documentation as per section 4.1	10 working days from the completion of phase 1
Intra-Rack Cable Management System	45 calendar days from contract award
Spare Parts Kits	10 working days from initial acceptance of the rack (CLIN) to which they pertain
Engineering Meeting Minutes	As Required
Engineering Artifacts	As Required/Requested
Server Baseline Configuration per server type for pre-approval	15 working days from contract award

4.1 Support Documentation Requirements – The following support documents are required to support this task and delivery:

Requirements	#	
Technical specification documentation must be delivered in PDF format for all materials and components thereof	227	P
Rack configuration maps must delivered in HTML format	228	P
Rack configuration maps must link to server and equipment configuration maps in HTML format	229	P

Final server and equipment configuration maps must link to the technical specs of each piece of equipment and any additional parts	230	P
Cable diagrams must be provided per server farm	231	P
All technical documentation delivered electronically must be on CD/DVD-ROM and delivered to both the JEOD-KTOD-ACTD CTO	232	P
Electrical Diagrams must be provided per server farm	233	P
A template for development and delivery of all final maps, diagrams and tech specs must be pre-approved before final delivery	234	P
Final Component Baseline Configuration Documentation (broken down by rack, Hardware/software and element) must be provided	235	P
A final storage and FS map must be provided per server farm	236	P

4.2 Materials Pre-Inspection Requirements

Requirements
All fully configured racks per CLIN will be pre-inspected by the offeror and COR prior to shipment or should physical discrepancies be found pertaining to rack configuration or the condition of the rack and its components, the vendor will assume all costs associated with the return of the rack, component or on-site correction of the discrepancy
Racks shall be inspected at the fabrication point

4.3 Materials Delivery Requirements

Requirements
Only appropriate JEOD representatives can sign for delivery when items delivered to NAVEODTECHDIV (list of approved representatives will be provided by the government
Under NO circumstances can a government contractor sign for final delivery of any items to NAVEODTECHDIV
Under NO circumstances will signed delivery be considered acceptance
All racks with the possible exception of power distribution racks will be prefabricated with all components (racking, cable management, intra rack cables, servers and other hardware), except for those preinstalled components indicated in Diagram 1 that the vendor is not responsible for.
All materials should be addressed to: ITC (SW) Robert J. Gaskill ACTD DET BLDG 2172 NAVEODTECHDIV 2008 Stump Neck RD Indian Head MD 20640 For final delivery to NAVEODTECHDIV

In the event of the demise of the contractor, the contractor shall make available to the Government the documentation/data rights necessary to produce and support the current delivered components as well as spare and repair parts.

4.4 Labor

The government accepts the fact that certain installation tasks cannot be completed therefore final acceptance tests cannot be conducted until the current server farms are set out of service and the migration phase set forth under phase 2 (option 1) of this SOW is executed. In lieu of this fact, the following concessions must be made by the government;

Labor required for the completion of phase 1 while executed and charged during phase 2 will not be drawn from the pool of labor required to meet the requirements of phase 2 as these efforts overlap but are not intertwined.

5. Phase 2 Tasks, Requirements and Deliverables

5.1 Tasks - The contractor shall deliver the materials outlined in this phase, and will provide 300 hours worth of on-site technical support to assist the government with the migration of all data, services and applications currently residing on the 2 existing server farms onto the 2 new farms covered under phase 1. Labor in support of phase 1 tasks shall not be applied against this pool of labor.

5.1.1 Data Migration - The contractor will assist with the development, planning and implementation of the logical configuration of all storage and backup systems within both server farms. This effort will be coordinated with JEODNET System Administrators. The configuration and implementation plans for these systems must be approved by the JEOD-KTOD-ACTD CTO prior to implementation. The contractor will assist JEODNET System Administrators with the physical migration of data form existing storage systems onto the new systems covered under section 2, and will assist with placing the old systems out of service. The contractor will document the final configuration of all storage and backup systems prior to final acceptance and perform acceptance testing with JEODNET System Administrators. Only the JEOD-KTOD-ACTD CTO can sign for final acceptance

5.1.2 Service/Application Installation - The contractor will support JEODNET System Administrators with the installation and migration of advanced services and applications from the old server farms to the 2 new farms covered under phase 1 and the removal of the old server farms from active service. The contractor is not responsible for designing the implementation of these services/applications however, the contractor is responsible of assisting the government with the migration of these services/applications from the old farms to the new farms under the supervision and direction of JEODNET System Administrators. These Services/Applications include

- ?? DNS
- ?? DHCP
- ?? Certificate Services
- ?? Exchange Server 2003
- ?? Oracle 9i
- ?? SQL 2000
- ?? RIS
- ?? Active Directory
- ?? RAS

5.1.3 Final acceptance of Phase 1 - The contractor is responsible for installing services and applications set forth in phase 1 but deferred to this phase, and conducting all final acceptance test that could not be performed during phase 1 due to incomplete configuration. Final acceptance for all phase 1 materials and tasks will occur during this phase as per the approved acceptance plan. The government shall not be charged for labor related to this task and the hours required to complete this task will not count against the 300 hour pool. Installation and configuration hours required to enable the completion of this task must be charged against the applicable phase 1 CLIN. Should the government choose not to exercise option 1 initial acceptance under phase 1 will be considered final acceptance

5.1.4 Update Support Documentation – The contractor shall update all support documentation to reflect the server and service configuration additions / changes that occurred during phase 2.

5.2 Materials & Requirements – The following software shall be provided under this phase

Oracle 9i Enterprise – QTY 2 licensed per CPU
Microsoft Exchange Server 2003 Enterprise Edition – QTY 2 No CAL licenses required
Microsoft SQL Server 2000 Enterprise Edition – QTY 2

5.3 Deliverables

Deliverable	Scheduled Delivery Date
Software Licenses	10 working days from DO per CLIN
Final SAN Configuration Documentation	10 working days from end of phase 2
Final Acceptance Test Documentation	10 working days from the end of phase 2
Updated Equipment Configuration Documentation	10 working days from the end of phase 2
Updated Rack configuration maps	10 working days from the end of phase 2
Meeting Minutes	As required

5.4 Labor - the following labor categories are anticipated to support solution engineering and materials installation during this phase of procurement. Refer to the Key Personnel Qualifications document for a list of minimum qualifications per category

- System Administrator – Storage Solutions Specialist
- Network Engineer – MSCE
- Project Manager

6. Phase 3 Tasks, Requirements and Deliverables (Option I)

6.1 Tasks

6.1.1 The contractor will architect, implement and operationally test an enterprise management system for both JEODNET's NIPRNET and SIPRNET enclaves as per the requirements set forth in this section.

6.1.2 The contractor will architect, implement and operationally test an enterprise intrusion detection system for JEODNET's NIPRNET enclave only, as per the requirements set forth in this section

6.2 Requirements

6.2.1 Enterprise Management System

Requirements	#	
Enterprise management software shall be capable of monitoring the status of all equipment covered by phases 1 and 4 and software covered phases 1, 2 and 4 of this SOW	237	P
System will be capable of monitoring and managing equipment at other nodes	238	P
System will not use SNMP to monitor items covered by phase 1 and 4	239	P
System will be capable of using SNMP to monitor equipment not covered by this procurement	240	P
System will consist of an intuitive visual UI for displaying a network map and the status of the equipment on that map	241	P
System must be demonstrated to and approved by the JEOD-KTOD-ACTDs CTO prior to procurement	242	P
System must be capable of monitoring Oracle 9i	243	P
System must be capable of monitoring Exchange Server 2003	244	P
System must be capable of monitoring all variants of Microsoft Windows Server 2003 covered by phases 1 and 4	245	P
System must be capable of monitoring SQL 2000 server	246	P
System must be capable of monitoring network traffic and saturation	247	P
System must be capable of monitoring the power distribution racks	248	P
System must be compatible with ALTIRIS for managing and monitoring workstations	249	P
System must be capable of establishing service maps and monitoring the services provided by JEODNET	250	P
System must contain or be able to feed upstream help desk service related software	251	P
Support agreements will conform to section 3.7	252	P
System must be capable of audit log reduction	253	P

6.2.2 Intrusion Detection

Requirements	#	
System must be able to query, concatenate and analyze the activity of various system event and security logs	254	P
System must be able to profile network activity	255	P
System must be able to match network attack activity profiles to actual network activity	256	P
System must be able to detect intrusion related activity	257	P
System must be able to initiate configurable responses to suspected attacks or intrusion activity	258	P
System must support tiered levels of response	259	P
System must be capable or remote notification of SYS ADMIN personnel	260	P
System must support evidence collection pertaining to intrusion activity	261	P
System must be capable of initiating hostile/active responses to and toward entities conducting a	262	P

suspected attack		
System must be demonstrated to and approved by the JEOD-KTOD-ACTDs CTO prior to procurement	263	P
Support agreement will conform to section 3.7	264	P
System must be capable of audit log reduction	265	P

6.3 Deliverables

Deliverable	Scheduled Delivery Date
Enterprise Management System	30 calendar days from the time the DO is issued for the CLIN
Enterprise Management System Modules	7 calendar days from the time DO is issued for the CLIN
Intrusion Detection System	30 calendar days from the time the DO is issued for the CLIN
Intrusion Detection System Modules	7 calendar days from the time the DO is issued for the CLIN
Support Documentation for the Enterprise Management System and Intrusion Detection System	5 working days from the completion of phase 3
Configuration Documentation for the Enterprise Management System and Intrusion Detection System	5 working days from successful completion of the Operational Acceptance Test
Meeting Minutes	As required
Architecture/Engineering Artifacts	As required or requested

Sections 4.2 and 4.3 apply to all deliverables under this phase.

7. Phase 4 Tasks, Requirements and Deliverables (Option II)

7.1 Tasks - The contractor will deliver, install (on-site) and baseline configure materials for 4 regional gateway sties (each site having a NIPRNET and SIPRNET Implementation) as outlined by the following requirements.

7.2 Requirements

7.2.1 Gateway Implementation (Note: Each gateway contains a physically separate but identical NIPRNET and SIPRNET implementation. All implementations at all gateway node locations are to be identical. For clarity this means there will be 8 actual implementations. These requirements define the minimum technical specifications for 1 implementation as all 8 are to be the same)

Requirements	#	
Each implementation must fit in no more than 3 42U high racks with a 28" FUNCTIONAL SERVER depth	266	P
Racks must comply with section 3.4 with the exception of upstream KVM & Power management requirements and gateway racks must be environmentally controlled	267	P
Gateway must contain a UPS unit that is capable of providing 45 minutes of battery life, power distribution, conditioning and surge suppression for all equipment in the racks	268	P
Each Gateway must contain 2 24 port 100baseT Nortel Bay Stack switches (or equivalent) that are capable of port teaming (see ancillary equipment under phase 1)	269	P
Each Gateway must contain 2 Nortel Alteon Firewall devices or equivalent (see ancillary equipment under phase 1)	270	P
Each firewall device must use checkpoint firewall software or equivalent and subscribe to the enterprise firewall management software (IDS) at N1 (see ancillary equipment under phase 1)	271	P
Each Gateway must contain 2 (NSA Certified) SafeNet Red Eagle HAIPE VPN gateway (see ancillary equipment under phase 1)	272	P
Each VPN gateway device will subscribe to enterprise VPN management software at N1	273	P
Each Gateway must contain 5 type 1 servers	274	P
Each Gateway must contain 3 type 2 servers	275	P
Each Gateway must contain 2 F5 3DNS Servers with Big IP	276	P
Each Gateway must contain 1 Enterprise Storage System with a minimum of 40 TB Usable capacity (scalable to 100TB usable)	277	P
Storage system can be either Fiber Channel, SCSI or ATA and must support Raid 5	278	P
Storage system must contain redundant power supplies for all components	279	P
Storage System Raid controller must contain redundant cache of the largest capacity supported	280	P
Storage system must connect using 100% redundant paths to the type 1 server cluster and type 2 server	281	P
All servers will attach to their appropriate switch (information to be provided after contract award) using 2 100baseT teamed NICS	282	T
Spare parts kits must be provided as defined under section 3.4	283	P
Cable labeling and management must conform to section 3.5.4	284	P
All Hardware must be physically installed and cabled within the rack	285	P
All materials must be covered by technical support and warranties as defined in section 3.6	286	P
Each implementation must make use of enterprise management system and enterprise intrusion detection system as defined in section 6	287	P

F5 3 DNS Mandatory configuration (QTY-2 per gateway)

Part #	**Description**
F5-3DNS	A339294 3-DNS Controller 520

F5-SVC-BIG-PRE	A339234 Annual Premium Service-5
F5-INST-BIG-1	A255681 Install/Config - Basic Products

7.3 Deliverables

Deliverable	Scheduled Delivery Date
N3.1 NIPRNET Gateway Node	45 calendar days from issue of DO against this CLIN
N3.1 SIPRNET Gateway Node	45 calendar days from issue of DO against this CLIN
N3.2 NIPRNET Gateway Node	45 calendar days from issue of DO against this CLIN
N3.2 SIPRNET Gateway Node	45 calendar days from issue of DO against this CLIN
N3.3 NIPRNET Gateway Node	45 calendar days from issue of DO against this CLIN
N3.3 SIPRNET Gateway Node	45 calendar days from issue of DO against this CLIN
N3.4 NIPRNET Gateway Node	45 calendar days from issue of DO against this CLIN
N3.4 SIPRNET Gateway Node	45 calendar days from issue of DO against this CLIN
Support documentation as per section 4.1	10 working days from acceptance of node implementation.
Meeting Minutes	As Required
Engineering / Architecture Artifacts	As required / requested
Applicable Software/Hardware Licenses and activation codes organized and delivered with original installation media (and a master listing of all installation and activation codes) as a package	45 Calendar days from issue of DO against the associated gateway node CLIN
Cable Labeling Plan for final approval	10 working days from contract award
Template for delivery of final support documentation for approval	10 working days from contract award
Spare Parts Kits	60 calendar days from issue of DO against the associated gateway node CLIN

Sections 4.2 and 4.3 apply to all deliverables under this phase with the exception of the delivery address. Materials will be shipped directly to the gateway sites. Addresses will be provided to the contractor when this option and the appropriate CLINs within are exercised/procured by the government.

7.4 Labor – the following labor categories are anticipated to support solution engineering and materials installation during this phase of procurement. Refer to the Key Personnel Qualifications document for a list of minimum qualifications per category.

- System Administrator – Storage Specialist
- System Administrator – Server Hardware Specialist
- System Administrator - General
- Network Engineer – MSCE
- Project Manager

8.0 Government Furnished Property/Material (GPM/GFM) - The government will furnish publications, forms and other documentation as necessary for the contractor to perform under this Statement of Work. If the contractor works on government site, the government will provide paper and other consumable office supplies used at government facilities. If the contractor works on the government site, the government will make available for contractor use furnishings, computer and networking capabilities, and service provider agreements to support the tasks described in this SOW. Aspects of the JEODNET are classified. Upon verification of contractor clearances, the government will provide access on a need to know basis to information. The highest level of classified information pertaining to the JEODNET is Secret.

9.0 Security - The highest level of classified information processed by the JEODNET is Secret. All Contractor Personnel shall be US Citizens moreover, they shall speak English fluently. Additionally all personnel associated in any way with any task covered by this SOW will possess at a minimum secret level clearance upon task start date.

10.0 Hours will normally be 8 hours per day, 5 days per week, and may include Government holidays. Contractor personnel shall not work more than 40 hours per week however, work may be conducted during any time of the day therefore a 9a-5p schedule is not implied nor will work performed outside these hours be grounds for overtime.

11.0 Travel – Travel to NAVEODTECHDIV and overseas will be required. Personnel assigned to overseas travel shall be fluent in English, able to gain access to any country, and possess a current US passport. Travel is anticipated as follows

Phase 1 – Estimate adequate travel to support all on-site tasks at NAVEODTECHDIV

Phase 2 – Estimate adequate travel to support all on-site tasks at NAVEODTECHDIV

Phase 3 – Estimate adequate travel to support all on-site tasks at NAVEODTECHDIV

Phase 4 – Estimate travel adequate to support 1 week on-site to support the delivery and installation of material CLINS in the 4 regions stated under phase 4 (Asia-Japan, Europe-Italy, Hawaii-Ohau, and the Middle East-Bahrain).

Security Requirements Traceability Matrix
for
JEODNET

Levels of Concern - Integrity

DCID Para	Stated Requirement	C&A Evaluation
5.B.2.a.3	[Change1] [A system operating at the Medium Level-of-Concern for integrity shall implement] Change Control that includes: a. Mechanisms that notify users of the time and date of the last change in data content. b. Procedures and technical system features to assure that changes to the data or to security-related items are: 1. Executed only by authorized personnel. 2. Properly implemented.	
Initiative Implementation	The Windows OS keeps track of the date and time of last modification of data files. DAC file protections can be set to restrict modifications to authorized personnel. Changes to data files are audited as well.	
5.B.2.a.4	[CM1] [A system operating at the Medium Level-of-Concern for integrity shall implement] Configuration Management (CM) that includes: a. Policies that assure the effectiveness of storage integrity. b. Procedures to assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software.	
Initiative Implementation	The JEODNET CM Plan addresses maintaining version control of software, firmware, and hardware for deployed systems. The JEODNET CCB must approve all changes made to the baseline software. The HF CCB approves changes made to the configuration deployed for HF. In addition, logs are kept to document all maintenance activities, including changes to configuration files.	
5.B.2.a.5	[CM2] [A system operating at the Medium Level-of-Concern for integrity shall implement] Configuration Management that includes: a. A CM Plan, including: 1. Policies that assure storage integrity. 2. Procedures for identifying and documenting system connectivity, including any software, hardware, and firmware used for all communications (including, but not limited to wireless, IR, etc.). 3. Procedures for identifying and documenting the type, model, and brand of system or component, security relevant software, hardware, and firmware product names and version or release numbers, and physical locations. b. A CM process to implement the CM Plan.	
Initiative Implementation	The JEODNET Enterprise SSAA calls out the CM Plan and all other policy documents that define the policies and procedures for maintaining software configuration control for JEODNET. The Enterprise SSAA identifies the software, hardware and firmware versions for the Enterprise deployed system and the Node SSAA package calls out these products as implemented at every node location. Changes to the deployed system must be approved by the JEODNET CCB.	
5.B.2.a.6	[Integrty2] [A system operating at the Medium Level-of-Concern for integrity shall implement] Data and software storage integrity protection, including the use of strong integrity mechanisms (e.g., integrity locks, encryption).	
Initiative Implementation	Storage integrity is provided by the NTFS journaling file system under Windows.	
5.B.2.a.7	[Integrty3] [A system operating at the Medium Level-of-Concern for integrity shall	

DCID Para	Stated Requirement	C&A Evaluation
	implement] Integrity, including the implementation of specific non-repudiation capabilities (e.g., digital signatures), if mission accomplishment requires non-repudiation.	
Initiative Implementation	Digital signatures are used to cryptographically bind the label markings to the data for transmission over web services. This provides both source authentication and validates the message integrity.	
5.B.2.a.8	[MalCode] [A system operating at the Medium Level-of-Concern for integrity shall implement] Procedures to prevent the introduction of malicious code into the system, including the timely updating of those mechanisms intended to prevent the introduction of malicious code (e.g., updating anti-viral software).	
Initiative Implementation	Norton Antivirus Corporate is installed and run on all JEODNET servers. Virus protection is regularly updated. Access to removable media is limited to privileged users. For further details refer to the JEODNET Enterprise SSP and Enterprise Contingency Policy, for detailed information on implementation at any node location refer to the SSAA appendix and contingency plan for the node site.	
5.B.2.b.1	[Validate] [The following assurance shall be provided for a system operating at a Medium Level-of-Concern for Integrity:] Security Support Structure Validation, including procedures or features to validate, periodically, the correct operation of the hardware, software, and firmware elements of the Security Support Structure.	
Initiative Implementation	Security test plans and procedures are developed. Tests are performed as part of security accreditation. In addition, periodic ISS scans are performed to ensure security patches are installed and security features are performing correctly. Audit review provides additional assurance. Responsibility for initiating and tracking updates resides with the JEODNET Enterprise Management System	
5.B.2.b.2	[Verif1] [The following assurance shall be provided for a system operating at a Medium Level-of-Concern for Integrity:] Verification by the ISSM that the necessary security procedures and mechanisms are in place; testing of them by the ISSM to ensure that they work appropriately.	
Initiative Implementation	Security test plans and procedures are developed. Security tests are performed and results verified by the CTO and DAA for new releases of the software/hardware.	

Levels of Concern - Availability

DCID Para	Stated Requirement	C&A Evaluation
6.B.2.a.1	[Avail] [A system operating at the Medium Level-of-Concern for Availability shall implement] Processes and procedures to allow for the restoration* of the system. [*Restoration of service is a necessary function to guard against both natural disasters and denial-of-service attacks.]	
Initiative Implementation	JEODNET is installed on multiple redundant servers so functionality can be quickly restored by automatic failover where configured or modifying the configuration to run on the alternate server. The original server can then be repaired or reinstalled and either be switched back to or remain as an alternate server.	
6.B.2.a.2	[Backup3] [A system operating at the Medium Level-of-Concern for Availability shall implement] Backup storage that is located to allow the prompt restoration of data. If required by the DAA, there shall additionally be off-site backup storage of the data, as per approved SSP; such storage is intended to enable recovery if a single event eliminates both the original data and the on-site backup data. If regular off-site backup is not feasible, as, for example, on a ship at sea, alternative procedures, such a secure transmission of the data to an appropriate off-site location, should be considered.	
Initiative Implementation	The JEODNET software, data and configuration files can be quickly restored from the installation CD or from the Enterprise Distributed Backup System.	
6.B.2.a.3	[Backup5] [A system operating at the Medium Level-of-Concern for Availability shall implement] Backup procedures to allow the restoration of operational capabilities with minimal loss of service or data. These procedures shall require: a. Frequent backups of data. b. To the extent deemed necessary by the DAA, assurance that the system state after the restore will reflect the security-relevant changes to the system between the backup and the restore. c. Assurance that the availability of information in storage is adequate for all operational situations, and that catastrophic damage to any single storage entity will not result in system-wide loss of information. These policies shall include, among others, procedures for ensuring the physical protection of operational and backup media and equipment, and for ensuring the continued functionality of the operational and backup media and equipment. d. Restoration of any security-relevant segment of the system state (e.g., access control lists, cryptologic keys, deleted system status information) without requiring destruction of other system data.	
Initiative Implementation	The JEODNET software, data and configuration files can be quickly restored from the installation CD or from the Enterprise Distributed Backup System. No data is considered perishable.	
6.B.2.a.4	[Commun] [A system operating at the Medium Level-of-Concern for Availability shall implement] Communications capability that provides adequate communications to accomplish the mission when the primary operations communications capabilities are unavailable.	
Initiative Implementation	JEODNET is completely dependent on the NIPRNET and SIPRNET/NIPRNET. However JEODNET employs redundant communications circuits between all key infrastructure node locations and all server equipment within those locations. JEODNET has engineered for no single point of failure on the network level (does not include workstations) at all Key infrastructure sites (N1, N2 and all N3s)	
6.B.2.a.5	[Maint] [A system operating at the Medium Level-of-Concern for	

DCID Para	Stated Requirement	C&A Evaluation
	Availability shall implement] Maintenance procedures that include preventive maintenance, scheduled to maximize the availability of the system, and thus to minimize interference with the operation of the system. Planning for maintenance shall include at least: a. On-call maintenance. b. On-site diagnostics. c. Control of Remote Diagnostics, where applicable. (See para. 8B.8.d, for a discussion of remote diagnostics.)	
Initiative Implementation	JEODNET will provide installation and maintenance guides for the system. Maintenance and diagnostics will be performed both automatically by the Enterprise Management System and manually by support personnel at the site of deployment.	
6.B.2.a.6	[Power1] [A system operating at the Medium Level-of-Concern for Availability shall implement] System Availability, including, by default for a multi-user system, conditioned, battery-backed power adequate to allow the system to be fail-soft. If the system is multi-user, the decision not to use an Uninterruptible Power Supply (UPS) for the system shall be explicit.	
Initiative Implementation	JEODNET servers will use 3 tiers of power protection 1. A and B side power 2. Backup generator capable of sustaining 8 hours of data center operations 3. an UPS system to allow time for graceful system shutdown initiated by the UPS system on all equipment that can accept shutdown commands from the UPS system.	
6.B.2.a.7	[Power2] [A system operating at the Medium Level-of-Concern for Availability shall implement] System Availability, including, as required by the DAA, procedures for graceful transfer of the system to an alternate power source; these procedures shall ensure that the transfer is completed within the timing requirements of the application(s) on the system.	
Initiative Implementation	N1 and N2 will have A/B power and backup generators. Alternate power at N3 sites and beyond will depend on site location.	
6.B.2.a.8	[Recovery] [A system operating at the Medium Level-of-Concern for Availability shall implement] Recovery procedures and technical system features that assure that system recovery is done in a trusted and secure manner. If any circumstances can cause an untrusted recovery, such circumstances shall be documented and appropriate mitigating procedures shall be put in place.	
Initiative Implementation	Analysis is performed to ensure that JEODNET recovers in a trusted state. Recovery is a function of both the Enterprise Management System, Enterprise Intrusion Detection System and the Distributed Backup System	
6.B.2.b.1	[Cont1] [The following assurance shall be provided for a system operating at a Medium Level-of-Concern for Availability:] Contingency Planning that includes a Contingency/Disaster Recovery Plan.	
Initiative Implementation	Contingency planning is part of an overall risk management plan which must be instituted for all of JEODNET and its deployment locations. Refer to the Enterprise Contingency policy or specific node Contingency Plan	
6.B.3.a.2	[Backup4] [A system operating at the High Level-of-Concern for Availability shall implement] Backup procedures, including: a. A capability to conduct backup storage and restoration of data. b. Frequent backups of data.* c. At least annual restoration of backup data. d. Backup storage that is located to allow the immediate restoration of	

DCID Para	Stated Requirement	C&A Evaluation
	data. There shall additionally be off-site backup storage of the data, as per approved SSP; such storage is intended to enable recovery if a single event eliminates both the original and the on-site, backup data. If regular off-site backup is not feasible, as, for example, on a ship at sea, alternative procedures such as secure transmission of the data to an appropriate off-site location, should be considered. [*In this context, frequent means after any significant system hardware, software, or firmware change, and, in any case, no less often than once per year.]	
Initiative Implementation	The Enterprise Distributed Backup System handles backup and restoration for all assets in the enterprise considered to contain non-perishable data, leveraging the combination of the high capacity SANs and NAS solutions within the enterprise. This system backs up all data and systems locally as well as remotely and distributes copies of these backups automatically to other enterprise node locations over the HAPIE conformant VPN tunnels within the network.	
6.B.3.a.4	[Backup6] [A system operating at the High Level-of-Concern for Availability shall implement] Backup procedures, including: a. Assurance that the system state after the restore will reflect security-relevant changes to the system between the backup and the restore. b. Consideration to the use of technical features that enhance data integrity and availability including, among others, remote journaling, Redundant Array of Inexpensive Disks (RAID) 1 and above, and similar techniques.	
Initiative Implementation	When security relevant modifications are made to configuration files, those files are snap-shot and backed up via the Enterprise Distributed Backup System.	
6.B.3.a.6	[DOS] [A system operating at the High Level-of-Concern for Availability shall implement] Prevention of Denial of Service Attacks.* Where technically feasible, procedures and mechanisms shall be in place to curtail or prevent well-known, detectable, and preventable denial of service attacks (e.g., SYN attack). [*Only a limited number of denial-of-service attacks are detectable and preventable. Often, prevention of such attacks is handled by a controlled interface. (See Chapter 7 for a discussion on controlled interfaces.)]	
Initiative Implementation	This is handled by the Enterprise Firewalls and Enterprise Intrusion Detection System. This system also collects evidence data and where configured launches counter attacks to subvert the attack	
6.B.3.a.8	[Monit] [A system operating at the High Level-of-Concern for Availability shall implement] Periodic testing by the ISSO or ISSM of the security posture of the IS by employing various intrusion/attack detection and monitoring tools. The ISSO/M shall not invoke such attack software without approval from the appropriate authorities and concurrence of legal counsel. The monitoring tools shall be used for the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns.	
Initiative Implementation	This is a function of the Enterprise Management and Intrusion Detection Systems and is monitored by JEODNET System Administrators	
6.B.3.a.11	[Priority] [A system operating at the High Level-of-Concern for Availability shall implement] Priority protection that includes no "Deny Up" (i.e., a lower-priority process shall not be able to interfere with the system's servicing of any higher-priority process).	
Initiative Implementation	The Windows OS supports process prioritization. Invocation of processes on JEODNET servers is restricted to privileged users so threat is limited	
6.B.3.b.2	[Cont2] [The following assurance shall be provided for a system operating at a High Level-of-Concern for Availability:] Contingency Planning, including:	

DCID Para	Stated Requirement	C&A Evaluation
	a. Adequate hardware, firmware, software, power, and cooling to accomplish the mission when the operational equipment is unavailable. Consideration shall be given to fault-tolerant or "hot-backup" operations. The decision whether or not to use these techniques shall be explicit. b. Regular exercising and testing of the contingency plans. The plans for the tests shall be documented in the Contingency/Disaster Recovery Plan.	
Initiative Implementation	JEODNET supports contingency planning by allowing failover to redundant software on alternated hardware. Refer to the Enterprise Contingency Policy and node contingency plans.	

Controlled Interface

DCID Para	Stated Requirement	C&A Evaluation
7.B.2 [NRO a]	NRO - Enclave Security Policy - *Controlled interfaces must be able to enforce a documented enclave security policy. Each enclave shall have a documented security policy.* Each enclave must define who (e.g. clearances, accesses, citizenship) can access data within the enclave and specify the set of rules the controlled interface must enforce. Each controlled interface shall be able to enforce a documented enclave security policy. For each enclave, providers shall define the authorized services provided, protocols employed, and information flow through the controlled interface. NOTE: Protocols and services are not interchangeable. A file transport service may be authorized using Secure FTP but not Anonymous FTP. Also one service may be embedded within another services, e.g., a file transport service provided by a mail-with-attachments services using the Secure MIME protocol.	
Initiative Implementation	Firewalls will be configured to enforce the deployment site's enclave security policy JEODNET provides a controlled interface by either requesting a PKI certificate or username and password which can be authenticated for identification and role in LDAP. In addition, the JEODNET Web Services provide Role-Based Access Control restricting which users may access them using Security Services.	
7.B.2 [NRO b]	NRO - Controlled Interface Security Policy - *Controlled interface implementation(s) must be defined in accordance with an enclave security policy.* Providers shall implement controlled interfaces in accordance with a detailed security concept of operations and a security plan. The enclave security policy and the set of approved services for each controlled interface shall be documented in the CM plan. Information to be included in a controlled interface security policy: - Purpose and objective of controlled interface - Source /Destination sub-networks and/or host systems - Authorized services (protocols) permitted through the controlled interface per the enclave security policy - Policy for access by authorized users from external locations - Sensitivity level of the information - Handling caveats - Identification of direct and indirect users - User need-to-know, authorization, and clearances - Identification of data owner(s) - Mission criticality - Requirements for integrity and availability	
Initiative Implementation	Firewalls and the Enterprise Intrusion Detection System will be configured to enforce the deployment site's enclave security policy. LDAP entries will identify valid users and their roles. Modifications of JEODNET configuration files are restricted to privileged users.	
7.B.2.a.1	Controlled Interface Modifications - [The DAA shall ensure that] Mechanisms or procedures exist to prohibit general users from modifying the functional capabilities of the Controlled Interface.	
Initiative Implementation	Firewalls, LDAP entries, and JEODNET configuration files can only be configured by authorized personnel.	
7.B.2.a.2	Controlled Interface Monitoring - [The DAA shall ensure that] Automated mechanisms are employed that can monitor the Controlled Interface for symptoms of failure or compromise. The mechanisms shall be protected against failure or compromise.	
Initiative Implementation	This is a function of the Enterprise Managements System and Enterprise Intrusion Detection System	
7.B.2.a.3	Controlled Interface Protection - [The DAA shall ensure that] The Controlled Interface is physically protected.	

DCID Para	Stated Requirement	C&A Evaluation
Initiative Implementation	Firewalls and servers will be inside the physical security of the deployment site and protected from access by unauthorized personnel.	
7.B.2.b	Routing Information Protection - Routing information, employed for either controlling the release of outgoing information or the delivery of incoming information, shall be supplied or alterable only by the Security Support Structure of the Controlled Interface.	
Initiative Implementation	Firewall configuration and LDAP entries are protected from alteration by unauthorized personnel.	
7.B.2.c	Controlled Interface Configuration and Location - Each Controlled Interface shall be configured and located to facilitate its ability to provide controlled communication between the interconnected systems.	
Initiative Implementation	Site dependent however, modifications can only occur in-band of the JEODNET VPN system.	
7.B.2.d	Controlled Interface Services - Each Controlled Interface shall be configured to ensure that all (incoming and outgoing) communications protocols, services, and communications not explicitly permitted are prohibited.	
Initiative Implementation	This is a function of both the Enterprise Firewalls and the Enterprise VPN system	
7.B.2.e	Controlled Interface Testing - Each Controlled Interface shall be tested to ensure that it satisfies all of the appropriate Controlled Interface criteria listed in this chapter.	
Initiative Implementation	JEODNET services are tested to ensure they are only accessible by valid users possessing the proper roles.	
7.B.2.f	Controlled Interface Configuration Management - The Controlled Interface shall be included in a configuration management program. Security policies, procedures, etc., shall be documented.	
Initiative Implementation	See the Enterprise SSAA Package and Node SSAA package appendices.	
7.B.2.g	Controlled Interface Safeguards - Safeguards shall be provided to assure that users cannot circumvent technical controls.	
Initiative Implementation	Web services cannot be accessed without going through the appropriate security services/systems.	
7.B.2.h	Controlled Interface Auditing - All direct user access to the Controlled Interface shall be audited.	
Initiative Implementation	All systems and services shall be audited. Audit reduction is a function of the Enterprise Management and Intrusion Detection Systems.	
7.B.2.i	Controlled Interface Remote Administration - Remote administration of the Controlled Interface is discouraged. All remote administration of Controlled Interfaces requires written approval of the DAA. If remote administration is employed, the session must be protected through the use of the following techniques: 1. Strong authentication, and either. 2. Physically separate communications paths, or. 3. Logically separated communications paths based upon either. a. NSA-approved encryption; or. b. NSA-approved encryption and DAA-approved privacy encryption to provide privacy of the remote administration session.	
Initiative Implementation	All remote admin will be 100% compliant with the JEODNET Remote Admin Policy	
7.B.2.i.4	Controlled Interface Access - Direct user access to the Controlled Interface shall require strong authentication.	
Initiative Implementation	Certificates or strong userID and Password shall be required	
7.B.3.c.1	Controlled Interface Traffic Review - [The Controlled Interface shall]	

DCID Para	Stated Requirement	C&A Evaluation
	Review the classification of all outgoing (i.e., going outside of the interconnected IS perimeter) traffic based on associated security labels (where provided) or data content (if applicable) before being released. If labels are used, the Controlled Interface must maintain the integrity of the labels.	
Initiative Implementation	Implementation of security services provides assurance that data classification is dominated by user's clearance.	
7.B.3.c.2	Controlled Interface Controlled Release - [The Controlled Interface shall] Ensure that only traffic that is explicitly permitted (based on traffic review) is released from the perimeter of the interconnected IS.	
Initiative Implementation		
7.B.3.c.3	Controlled Interface Encryption - [The Controlled Interface shall] Encrypt (as needed) all outgoing communication (including the body and attachment of the communication) with the appropriate level of encryption for the information, transmission medium, and target system.	
Initiative Implementation	SSL used to encrypt web service requests/responses.	
7.B.3.c.4	Controlled Interface Protection - [The Controlled Interface shall] Ensure that users and processes in a lower protection domain are prevented from accessing information for which they are not authorized that resides in a higher domain. In addition, when information at a higher security level is made available to a lower security level, the information shall be protected and maintained at the higher security level until it satisfies the traffic review and controlled release requirements described above. *IC The reference above to information at a higher security level being made available to a lower security level is interpreted as: ... When Information _In_ a higher security level is made available to a lower security level.*	
Initiative Implementation	Refer to cross domain policy and system documentation	
7.B.3.c.5	Controlled Interface Audit/Logging - [The Controlled Interface shall] Log all data release activities, to include identity of releaser, identity of recipient, identity of data released, device identifier (id) (e.g., port id), time, and date of release, modification, or application of security labels.	
Initiative Implementation	Security services log all web service calls as do the services themselves.	
7.B.3.c.6	Controlled Interface Fail-secure - [The Controlled Interface shall] Ensure that the operational failure of the Controlled Interface does not result in any unauthorized release of information outside of the IS perimeter.	
Initiative Implementation	If the security services fail, web services are unable to be invoked.	
7.B.3.d	Controlled Interface Availability Level of Concern - The Availability Level-of-Concern of each Confidentiality Controlled Interface shall be at least as high as the lowest Availability Level-of-Concern level of the interconnected ISs.	
Initiative Implementation	N/A	
7.B.3.e.1	Controlled Interface Accreditation - [In addition to the requirements imposed upon the Controlled Interface, each interconnected IS that is receiving information shall] Be accredited to process the level(s) and compartment(s) of information that it receives.	
Initiative Implementation	N/A	
7.B.3.e.2	Controlled Interface Feature and Assurances - [In addition to the	

DCID Para	Stated Requirement	C&A Evaluation
	requirements imposed upon the Controlled Interface, each interconnected IS that is receiving information shall] Provide the features and assurances necessary to ensure that information received is made available only to those authorized to receive the information.	
Initiative Implementation	N/A	
7.B.4.c	Controlled Interface Availability Level-of-Concern - The Availability Level-of-Concern of each Integrity Controlled Interface shall be at least as high as the Availability Level-of-Concern of the IS into which the information flows are directed.	
Initiative Implementation	N/A	
7.B.5	Controlled Interface Isolation and Protection - Unless the DAA provides a written exemption, the platform underlying the Controlled Interface mechanism must be able to isolate and protect the Controlled Interface application.	
Initiative Implementation	N/A	

Protection Levels 2 and 3

DCID Para	Stated Requirement	C&A Evaluation
4.B.2.a.1	[Access1] - [A system operating at Protection Level 2 shall employ] Access control, including: a. Denial of physical access by unauthorized individuals unless under constant supervision of technically qualified, authorized personnel. b. Procedures for controlling access by users and maintainers to IS resources, including those that are at remote locations.	
Initiative Implementation	Site dependent. JEODNET is deployed to secure facilities which provide physical access control. In addition, direct access to JEODNET servers is restricted to only privileged users possessing a local account.	
4.B.2.a.2	[Access2] - [A system operating at Protection Level 2 shall employ] Access Control, including a Discretionary Access Control (DAC) Policy. A system has implemented DAC when the Security Support Structure defines and controls access between named users and named objects (e.g., files and programs) in the system. The DAC policy includes administrative procedures to support the policy and its mechanisms. The enforcement mechanisms (e.g., self/group/public controls, access control lists, communities of interest [COIs], encryption) shall allow users to specify and control sharing of those objects by named individuals, or by defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The DAC mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.	
Initiative Implementation	Access to files on the JEODNET servers is DAC protected by the Windows NTFS. Only authorized users may modify these protections. Access to JEODNET web services is protected by role-based authentication provided by the Policy Decision Service based on LDAP entries.	
4.B.2.a.3	[AcctMan] - [A system operating at Protection Level 2 shall employ] Account Management procedures that include: a. Identifying types of accounts (individual and group, conditions for group membership, associated privileges). b. Establishing an account (i.e., required paperwork and processes). c. Activating an account. d. Modifying an account (e.g., disabling an account, changing privilege level, group memberships, authenticators). e. Terminating an account (i.e., processes and assurances).	
Initiative Implementation	User accounts are created on an individual basis. User accounts are assigned one or more roles. Privileges for a given user are determined by the role(s) assigned. Accounts can be administratively locked or terminated. Account management functionality is restricted to a minimal number of privileged users possessing appropriate role.	
4.B.2.a.4.a	[Audit1] - [A system operating at Protection Level 2 shall employ] Auditing procedures, including: Providing the capability to ensure that all audit records include enough information to allow the ISSO to determine the date and time of action (e.g., common network time), the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved.	
Initiative Implementation	Audit events are logged by the Windows OS. Each event identifies the action performed, date and time, user or process involved, and affected	

DCID Para	Stated Requirement	C&A Evaluation
	resources. Additional audit events are logged by the server applications and security services. Reduction of these logs is a function of the Enterprise Management and Intrusion Detection Systems	
4.B.2.a.4.b	[Audit1] - [A system operating at Protection Level 2 shall employ] Auditing procedures, including: Protecting the contents of audit trails against unauthorized access, modification, or deletion.	
Initiative Implementation	Read access, modification, archival, and deletion of audit records is restricted to Security Officers.	
4.B.2.a.4.c	[Audit1] - [A system operating at Protection Level 2 shall employ] Auditing procedures, including: Maintaining collected audit data at least 5 years and reviewing at least weekly.	
Initiative Implementation	This is a function of the Enterprise Management, Intrusion Detection and Distributed Backup Systems	
4.B.2.a.4.d	[Audit1] - [A system operating at Protection Level 2 shall employ] Auditing procedures, including: The system's creating and maintaining an audit trail that includes selected records of: 1. Successful and unsuccessful logons and logoffs. 2. Accesses to security-relevant objects and directories, including opens, closes, modifications, and deletions. 3. Activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users.	
Initiative Implementation	These events are all captured in the Windows Security Event Log.	
4.B.2.a.5.a	[Audit2] - [A system operating at Protection Level 2 shall employ] Auditing procedures, including: Individual accountability (i.e., unique identification of each user and association of that identity for all auditable actions taken by that individual).	
Initiative Implementation	The username or Distinguished Name (DN) of the responsible user is recorded for all audit events. These uniquely identify the user as shared accounts are not allowed by the security policy.	
4.B.2.a.5.b	[Audit2] - [A system operating at Protection Level 2 shall employ] Auditing procedures, including: Periodic testing by the ISSO or ISSM of the security posture of the IS by employing various intrusion/attack detection and monitoring tools. The ISSO/M shall not invoke such attack software without approval from the appropriate authorities and concurrence of legal counsel. The output of such tools shall be protected against unauthorized access, modification, or deletion. *IC A continuously running intrusion detection system is not required for AUDIT2. The tools referred to above are widely available commercial packages that will be run on a periodic, not continuous basis. These tools should be selected in coordination with your government representative.*	
Initiative Implementation	Site dependent.	
4.B.2.a.6	[Audit3] - [A system operating at Protection Level 2 shall employ] Auditing procedures, including:	

DCID Para	Stated Requirement	C&A Evaluation
	At the discretion of the DAA, audit procedures that include the existence and use of audit reduction and analysis tools.	
Initiative Implementation	Audit reduction and analysis is a function of the Enterprise Management and Intrusion Detection System	
4.B.2.a.7	[I&A2] - [A system operating at Protection Level 2 shall employ] An Identification and Authentication (I&A) management mechanism that ensures a unique identifier for each user and that associates that identifier with all auditable actions taken by the user. The following must be specified:* a. Initial authenticator content and administrative procedures for initial authenticator distribution. b. Individual and Group authenticators. (Group authenticators may only be used in conjunction with an individual/unique authenticator, that is, individuals must be authenticated with an individual authenticator prior to use of a group authenticator). c. Length, composition, and generation of authenticators. d. Change Processes (periodic and in case of compromise). e. Aging of static authenticators (i.e., not one-time passwords or biometric patterns). f. History of static authenticator changes, with assurance of non-replication of individual authenticators, per direction in approved SSP. g. Protection of authenticators to preserve confidentiality and integrity. [*Alternative controls, such as biometrics or smart cards, may be used at the discretion of the DAA. These alternative methods may have similar requirements. For example, the electronically stored version of biometric authentication patterns needs to be protected, as do password authenticators.]	
Initiative Implementation	An initial temporary password assignment is made at the time the account is created by the Security Officer and the system will require the user to change it upon the initial login. Group authenticators are not used in JEODNET. Passwords are configured to require a minimum of 8 characters, with at least 1 upper case character, 1 lower case character, 1 numeric, and 1 special character. Password aging is set to require new passwords be selected within 45 days. Password configuration parameters are set to prevent re-use of previous passwords (set to "remember" passwords indefinately). Passwords are encrypted for storage by the Windows OS.	
4.B.2.a.8	[I&A3] - [A system operating at Protection Level 2 shall employ] Identification and Authentication (I&A). Access to the IS by privileged users who either reside outside of the IS's perimeter or whose communications traverse data links (extranets, Internet, phone lines) that are outside of the IS's perimeter shall require the use of strong authentication (i.e., an I&A technique that is resistant to replay attacks).	
Initiative Implementation	Remote users are authenticated either by providing a valid DoD PKI or JEODNET certificate or username and password. The username or DN provided is looked up in LDAP for role and clearance information. Unknown users or users failing authentication (bad PKI cert or invalid password) are denied access to services. Remote users are not allowed access to privileged functionality. Security Officer and JEODNET Administrator functions can only be exercised by direct users.	
4.B.2.a.9	[I&A4] - [A system operating at Protection Level 2 shall employ] Identification and Authentication. In those instances where the means of authentication is user-specified passwords, the ISSO or ISSM may employ (under the auspices of the DAA) automated tools to validate that the passwords are sufficiently strong to resist cracking and other attacks	

DCID Para	Stated Requirement	C&A Evaluation
	intended to discover a user's password.	
Initiative Implementation	Strong PW checking is enabled.	
4.B.2.a.10	[LeastPrv] - [A system operating at Protection Level 2 shall employ] Least Privilege procedures, including the assurance that each user or process is granted the most restrictive set of privileges or accesses needed for the performance of authorized tasks shall be employed.	
Initiative Implementation	The roles granted a user determine his/her privileges and accesses. There are no super-user accounts. Account and audit management is restricted to an appropriate role. Installing and running JEODNET services is restricted to JEODNET Administrator role. Policy prevents assignment of both roles to same user.	
4.B.2.a.11	[ParamTrans] - [A system operating at Protection Level 2 shall employ] Parameter Transmission. Security parameters (e.g., labels, markings) shall be reliably associated (either explicitly or implicitly) with information exchanged between systems.	
Initiative Implementation	Each SOAP message (request and response) includes a label marking which is cryptographically bound to the message data via a digital signature.	
4.B.2.a.12	[Recovery] - [A system operating at Protection Level 2 shall employ] Recovery procedures and technical system features to assure that system recovery is done in a trusted and secure manner. If any circumstances can cause an untrusted recovery, such circumstances shall be documented and appropriate mitigating procedures shall be put in place.	
Initiative Implementation	There are currently no known circumstances in which the system will recover in an untrusted state. If any such possibility is discovered, it will be documented and mitigated.	
4.B.2.a.13	[ResrcCtrl] - [A system operating at Protection Level 2 shall employ] Resource Control. All authorizations to the information contained within an object shall be revoked prior to initial assignment, allocation, or reallocation to a subject from the Security Support Structure's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system. There must be no residual data from the former object.	
Initiative Implementation	Windows OS prevents object reuse by the implementation of "Subject/Object Residual Information Protection" as described in the Windows 2000 Common Criteria Security Target. STIG implementation also enables the wiping of the page file on reboot.	
4.B.2.a.14	[ScrnLck] - [A system operating at Protection Level 2 shall employ] Screen Lock. Unless there is an overriding technical or operational problem, a terminal/desktop/laptop screen-lock functionality shall be associated with each terminal/desktop/laptop computer. When activated, a screen-lock function shall place an unclassified pattern onto the entire screen of the terminal/desktop/laptop, totally hiding what was previously visible on the screen. Such a capability shall: a. Be enabled either by explicit user action or if the terminal/desktop/laptop is left idle for a specified period of time (e.g., 15 minutes or more). *IC Maximum Idle Time will be 15 minutes* b. Ensure that once the terminal/desktop/laptop security/screen-lock software is activated, access to the terminal/desktop/laptop requires knowledge of a unique authenticator. c. Not be considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).	
Initiative	After 3 minutes left idle, the user's screen is automatically locked. Entry	

DCID Para	Stated Requirement	C&A Evaluation
Implementation	of the user's password is required to unlock the screen. The user remains logged on. The screen lock only hides the display and prevents user keyboard or mouse inputs.	
4.B.2.a.15	[SessCtrl1] - [A system operating at Protection Level 2 shall employ] Session Controls, including: a. Notification to all users prior to gaining access to a system that system usage may be monitored, recorded, and subject to audit. Electronic means shall be employed where technically feasible. b. Notification to all users that use of the system indicates (1) the consent of the user to such monitoring and recording and (2) that unauthorized use is prohibited and subject to criminal and civil penalties. Electronic means shall be employed where technically feasible. *IC The appropriate Department of Justice approved warning statement will be displayed as part of the log-in process. This warning will be persistent and remain until the user takes positive action to acknowledge the content.*	
Initiative Implementation	The standard JEODNET warning banner is displayed prior to login by direct users. This banner contains the required warning information, and remains visible until acknowledged by the operator by a mouse click.	
4.B.2.a.16	[SessCtrl2] - [A system operating at Protection Level 2 shall employ] Enforcement of Session Controls, including: a. Procedures for controlling and auditing concurrent logons from different workstations. b. Station or session time-outs, as applicable. c. Limited retry on logon as technically feasible. d. System actions on unsuccessful logons (e.g., blacklisting of the terminal or user identifier).	
Initiative Implementation	Concurrent logins are not allowed. Session timeouts only result in a screen lock. After the third unsuccessful login authentication, the system disallows further attempts for a prescribed time period to inhibit automated password cracking.	
4.B.2.a.17	[Storage] - [A system operating at Protection Level 2 shall employ] Data Storage, implementing at least one of the following: a. Information stored in an area approved for open storage* of the information. b. Information stored in an area approved for continuous personnel access control (when continuous personnel access control is in effect), i.e., a 24-hour, 7-day-per-week operational area. c. Information secured as appropriate for closed storage. d. Information encrypted using NSA-approved encryption mechanisms appropriate (see paragraph 1.G.1) for the classification of stored data. [*In the context of storage confidentiality, "approved for open storage" must include consideration of the possibility of access by all users who have direct access to the system or network, wherever physically located.]	
Initiative Implementation	Site dependent. Current installations are in secure facilities approved for open storage.	
4.B.2.a.18.a	[Trans1] - [A system operating at Protection Level 2 shall employ] Data transmission that implements at least one of the following: 1. Information distributed only within an area approved for open storage of the information. 2. Information distributed via a Protected Distribution System* (PDS). 3. Information distributed using NSA-approved encryption mechanisms appropriate (see paragraph 1.G.1) for the classification of the information. 4. Information distributed using a trusted courier.	

DCID Para	Stated Requirement	C&A Evaluation
	[*A PDS provides physical protection or intrusion detection for communications lines. A PDS can also provide need-to-know isolation for communications lines.]	
Initiative Implementation	Information distribution is limited to NIPRNET and SIPRNET/NIPRNET, SIPRNET/NIPRNET is approved for transmission of data up to Secret NOFORN which is the highest level data handled by the system.	
4.B.2.a.18.b	[Trans1] - [For a system operating at Protection Level 2] Dial-up lines, other than those that are protected with nationally certified cryptographic devices or PDSs, shall not be used for gaining access to system resources that process intelligence information unless the DAA provides specific written authorization for a system to operate in this manner.	
Initiative Implementation	No access is allowed via dialup lines outside of the means spelled out in the JEODNET RAS Policy.	
4.B.2.b.1	[Doc1] - [For a system operating at Protection Level 2,] Documentation shall include: a. A System Security Plan (see Appendix C). b. A Security Concept of Operations (CONOPS). (The Security CONOPS may be included in the System Security Plan). The CONOPS shall at a minimum include a description of the purpose of the system, a description of the system architecture, the system's accreditation schedule, the system's Protection Level, integrity Level-of-Concern, availability Level-of-Concern, and a description of the factors that determine the system's Protection Level, integrity Level-of-Concern, and availability Level-of-Concern.	
Initiative Implementation	A System Security Plan has been produced for JEODNET and will be maintained, including the Security CONOPS.	
4.B.2.b.2	[Doc2] - [For a system operating at Protection Level 2,] Documentation shall include guide(s) or manual(s) for the system's privileged users. The manual(s) shall at a minimum provide information on (1) configuring, installing, and operating the system; (2) making optimum use of the system's security features; and (3) identifying known security vulnerabilities regarding the configuration and use of administrative functions. The documentation shall be updated as new vulnerabilities are identified.	
Initiative Implementation	Documentation to guide the privileged users can be found in the JEODNET Installation Guide and the System Security Plan.	
4.B.2.b.3	[Doc3] - [For a system operating at Protection Level 2,] The DAA may direct that documentation also shall include: a. Certification test plans and procedures detailing the implementation of the features and assurances for the required Protection Level. b. Reports of test results. c. A general user's guide that describes the protection mechanisms provided and that supplies guidelines on how the mechanisms are to be used and how they interact.	
Initiative Implementation	Certification test plans and procedures are contained in the System Security Plan. A test report is generated by the DAA representative as part of certification.	
4.B.2.b.4	[SysAssur1] - [For a system operating at Protection Level 2,] System Assurance shall include: a. Features and procedures to validate the integrity and the expected operation of the security-relevant software, hardware, and firmware. b. Features or procedures for protection of the operating system from	

DCID Para	Stated Requirement	C&A Evaluation
	improper changes.	
Initiative Implementation	The certification test procedures of the SSP can be run to validate the integrity and operation of security-relevant software. DAC file protections are used to protect the system from improper changes by restricting access to privileged users.	
4.B.2.b.5	[SysAssur2] - [For a system operating at Protection Level 2,] System Assurance shall include: a. Control of access to the Security Support Structure (i.e., the hardware, software, and firmware that perform operating system or security functions). b. Assurance of the integrity of the Security Support Structure.	
Initiative Implementation	Firmware is password protected and removable media booting is inhibited in the firmware. DAC file protections are used to protect the system the Security Support Structure by restricting access to privileged users. Audit review provides additional assurance of the integrity of the Security Support Structure.	
4.B.2.b.6	[Test2] - [For a system operating at Protection Level 2,] The ISSM shall provide written verification to the DAA that the system operates in accordance with the approved SSP, and that the security features, including access controls, configuration management, and discretionary access controls, are implemented and operational.	
Initiative Implementation	Written verification is provided after installation is performed and testing is completed.	
4.B.2.b.7	[Test3] - [For a system operating at Protection Level 2,] Additional testing, at the discretion of the DAA. a. Certification testing shall be conducted including verification that the features and assurances required for the Protection Level are functional. b. A test plan and procedures shall be developed and include: 1. A detailed description of the manner in which the system's Security Support Structure meets the technical requirements for the Protection Levels and Levels-of-Concern for integrity and availability. 2. A detailed description of the assurances that have been implemented, and how this implementation will be verified. 3. An outline of the inspection and test procedures used to verify this compliance.	
Initiative Implementation	Initial certification testing is performed in the development facility following the test plan and procedures of the SSP. Testing is also performed on the installed configuration at each operational site as per the test plan which contains a testing requirement traceability matrix that traces directly back to this matrix and the system requirements traceability matrix for all products.	
4.B.3.a.3	[Access3] - [A system operating at Protection Level 3 shall employ] Access Control, including: a. Some process or mechanism(s) that allows users (or processes acting on their behalf) to determine the formal access approvals (e.g., compartments into which users are briefed) granted to another user. This process or mechanism is intended to aid the user in determining the appropriateness of information exchange. b. Some process or mechanism(s) that allow users (or processes acting on their behalf) to determine the sensitivity level (i.e., classification level, classification category, and handling caveats) of data. This process or mechanism is intended to aid the user in determining the appropriateness	System is not at Protection Level 3.

DCID Para	Stated Requirement	C&A Evaluation
	of information exchange.	
Initiative Implementation	In HF04, LDAP entries for users included their citizenship and clearance info. All web service messages bore classification markings cryptographically bound to the data by the digital signature.	
4.B.3.a.7	[Audit4] - [A system operating at Protection Level 3 shall employ] An audit trail, created and maintained by the IS, that is capable of recording changes to the mechanism's list of user formal access permissions. (Note: Applicable only if the [Access3] access control mechanism is automated.)	System is not at Protection Level 3.
Initiative Implementation	Changes to LDAP audited.	
4.B.3.a.8.a	[Audit5] - [A system operating at Protection Level 3 shall employ] Auditing procedures, including: Individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual).	System is not at Protection Level 3.
Initiative Implementation	Audit records contain either username or DN of user.	
4.B.3.a.8.b	[Audit5] - [A system operating at Protection Level 3 shall employ] Auditing procedures, including: Periodic testing by the ISSO or ISSM of the security posture of the IS by employing various intrusion/attack detection and monitoring tools. The ISSO/M shall not invoke such attack software without approval from the appropriate authorities and concurrence of legal counsel. The output of such tools shall be protected against unauthorized access, modification, or deletion. These tools shall build upon audit reduction and analysis tools to aid the ISSO or ISSM in the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns.	System is not at Protection Level 3.
Initiative Implementation	This is a function of the Enterprise Intrusion Detection System.	
4.B.3.a.11	[I&A5] - [A system operating at Protection Level 3 shall employ] Identification and Authentication. In those instances where the users are remotely accessing the system, the users shall employ a strong authentication mechanism (i.e., an I&A technique that is resistant to replay attacks).	System is not at Protection Level 3.
Initiative Implementation	DoD PKI certificates or username/password prompts used for I&A.	
4.B.3.a.13	[Marking] - [A system operating at Protection Level 3 shall employ] Marking procedures and mechanisms to ensure that either the user or the system itself marks all data transmitted or stored by the system to reflect the sensitivity of the data (i.e., classification level, classification category, and handling caveats). Markings shall be retained with the data.	System is not at Protection Level 3.
Initiative Implementation	In HF04, all web service messages bore classification markings cryptographically bound to the data by the digital signature.	
4.B.3.a.18	[Separation] - [A system operating at Protection Level 3 shall employ] Separation of Roles. The functions of the ISSO and the system manager/system administrator shall not be performed by the same person.	System is not at Protection Level 3.
Initiative Implementation	Security Officer role is distinct from JEODNET Administrator role and are not assigned to same individual.	
4.B.3.b.6	[SysAssur3] - [For a system operating at Protection Level 3,] System Assurance shall include: a. Isolating the Security Support Structure, by means of partitions,	System is not at Protection Level 3.

DCID Para	Stated Requirement	C&A Evaluation
	domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions. b. Using up-to-date vulnerability assessment tools to validate the continued integrity of the Security Support Structure by ensuring that the system configuration does not contain any well-known security vulnerabilities.	
Initiative Implementation		
4.B.3.b.9	[Test4] - [For a system operating at Protection Level 3, the following additional] Testing, as required by the DAA [shall be conducted]: a. Security Penetration Testing shall be conducted to determine the level of difficulty in penetrating the security countermeasures of the system. b. An Independent Validation and Verification team shall be formed to assist in the security testing and to perform validation and verification testing of the system.	System is not at Protection Level 3.
Initiative Implementation	Certification testing performed by DAA representatives.	

Remaining Requirements

DCID Para	Stated Requirement	C&A Evaluation
7.B.4.b.2	Delivery - [The following integrity policy adjudication feature shall be provided:] Delivery. Ensure that incoming communications have an authorized user (and, as applicable, authorized addresses) as a destination.	
Initiative Implementation	Access is authenticated by the role checks performed by the Policy Decision Service.	
7.B.4.b.3	Filtering of Communications Protocols/Services - [The following integrity policy adjudication feature shall be provided:] Filtering. Support and filter communications protocols/services from outside the perimeter of the interconnected IS according to IS-appropriate needs (e.g., filter based on addresses, identity, protocol, authenticated traffic, and applications).	
Initiative Implementation	This is a function of the Enterprise firewalls and Enterprise Intrusion Detection System.	
7.B.4.b.4	Use of Proxies - [The following integrity policy adjudication feature shall be provided:] Proxies. Support, as appropriate, protocol-mediation software (i.e., proxies) that are able to understand and take protective action based on application-level protocols and associated data streams (e.g., filtering FTP connections to deny the use of the put command, effectively prohibiting the ability to write to an anonymous FTP server).	
Initiative Implementation		
7.B.4.b.5	Extensibility - [The following integrity policy adjudication feature shall be provided:] Extensibility. Where appropriate, provide security support for the incorporation of additional system services as they become available.	
Initiative Implementation	JEODNET has extensibility as a core tenet. New plug-in components can be easily added, and the security support is easily extended to new capabilities.	
7.B.4.b.7	Fail-Secure Mode - [The following integrity policy adjudication feature shall be provided:] Ensure that in the event of the operational failure of the Controlled Interface, no information external to the interconnected IS shall enter the IS.	
Initiative Implementation	If the security services/safeguards (PDS, cPDS, etc) fail, access will be denied.	
7.C.2.a.1	Web Client Certificates - All certificates* shall be protected via passwords that adhere to DAA guidelines and may be used in conjunction with some DAA-approved biometric mechanism. [*A certificate is an association between an identity and a public key. Certificates are used as a way to verify the authenticity of an organization or individual.]	
Initiative Implementation	Certificates are password/PIN-protected as issued by DoD or JEODNET.	
7.C.2.a.2	Use of Approved Certificate Authorities - Only DAA-approved certification authorities* shall issue certificates that are installed on ISs that process intelligence information. [*A Certification Authority is an organization that issues public key certificates.]	
Initiative Implementation	certificate authorities are DAA approved.	
7.C.2.a.3	Web Client Other Capabilities - If the Web client supports other capabilities (e.g., e-mail, collaborative computing, mobile code) in addition to traditional browser capabilities, then the use of these other capabilities shall be consistent with the appropriate guidelines stated elsewhere in this manual or as called for by the DAA.	
Initiative Implementation	Web clients are currently restricted to traditional browser capabilities.	

DCID Para	Stated Requirement	C&A Evaluation
7.C.2.b	Web Client Updates - In addition, as Web client updates that address known security flaws become available, the ISSO shall ensure that they are implemented as soon as possible.	
Initiative Implementation	This is a function of the Enterprise Management System	
7.D.2.a	External Server Location - External servers shall be located external to a site's Controlled Interface (e.g., firewall) or shall be on a network separate from the site's intranet.	
Initiative Implementation	All External Servers located at all nodes are in the JEODNET DMZ	
7.D.2.b	External Server Programs - The operating services and programs on servers (external and internal) shall be kept to a minimum, and services that are security risks (e.g., tftp, rlogin, rshell,) or not required shall be disabled.	
Initiative Implementation	Only necessary services are enabled on JEODNET servers. Risky services such as ftp and rlogin are disabled accept where approved by JEODNET policy in which case all instances are 100% policy compliant.	
7.D.2.c	Dedicated External Servers - The system that supports the server functionality shall, as much as possible, be dedicated to that purpose.	
Initiative Implementation	Each JEODNET server is dedicated to the services provided.	
7.D.2.d	External Server Security Patches - All operating system, protocol and application (e.g., FTP and Web) security patches shall be implemented as soon as possible after they become known and their functionality has been tested. *IC A log of applied patches shall be maintained for configuration management.*	
Initiative Implementation	Patches for vulnerabilities are implemented based on IAVA and other recommendations. Patch application is a function of the Enterprise Management System once approved for deployment by the JEODNET CMB.	
7.D.2.e	External Server Remote Access - Remote access to servers by privileged users requires the use of a strong authentication mechanism, and all such accesses shall be audited.	
Initiative Implementation	Privileged users are currently restricted to direct access to the servers or must be 100% compliant with the JEODNET remote administration policy.	
7.D.3.a	Public Servers - Public Servers. The information that is placed on a public server shall be limited to general access holdings that can be accessed by anyone who has authorized access to the inter/intranet/LAN on which the server resides. Servers employed as public servers shall implement all of the requirements stated in paragraph 7.D.2, above, and no general user accounts shall be permitted on the server.	
Initiative Implementation	JEODNET Public servers conform to para 7.D.2	
7.D.3.b.1	Restricted Access Servers Security Requirements - The underlying operating system shall satisfy the confidentiality requirements of Protection Level 2 or higher, integrity requirements for Basic Level-of-Concern or higher, and availability requirements for Basic Level-of-Concern or higher.	
Initiative Implementation	Servers are configured in accordance with appropriate STIGs to meet these security requirements.	
7.D.3.b.2	Restricted Access Servers Secure Web Technology - Web servers shall implement secure Web technology (e.g., Secure Sockets Layer, Secure HTTP) where capable.	
Initiative Implementation		

DCID Para	Stated Requirement	C&A Evaluation
7.D.3.b.3	Restricted Access Servers Authentication - Strong authentication shall be required for all users accessing the restricted servers, and all such accesses shall be audited.	
Initiative Implementation	Users are either prompted for username/password or must present a valid PKI certificate to gain access to the servers. All accesses are audited.	
7.E.5.a	Mobile Code Registration - All mobile code or executable content employed within an intelligence intranet enclave shall be registered within that enclave unless the DAA authorizes otherwise.	
Initiative Implementation	All mobile code is digitally signed and only signed code is allowed	
7.E.5.b	Mobile Code Review - As feasible, organizations shall implement a code review and quality control process for deployed mobile code or executable content and shall be responsible for the mobile code or executable content that they deploy.	
Initiative Implementation	All mobile code is subject to JEODNET CMB control and QA processes	
7.E.5.c	Mobile Code Deactivation - For those instances where there is no operational need to download mobile code or executable content, the ISSO or appropriate privileged user shall configure the IS or Controlled Interface to prevent the downloading of mobile code or executable content.	
Initiative Implementation	Only signed Mobile code from a JEODNET trusted source is allowed	
7.E.5.d	Mobile Code on Mission-critical Systems - Unless a written exception is granted by the DAA, organizations shall not run mobile code or executable content on mission-critical information systems.	
Initiative Implementation	Refer to Mobile Code Policy for JEODNET	
7.E.5.e	Mobile Code Download - Downloading of mobile code or executable content from a system that processes information of a different classification level shall only be permitted if a Controlled Interface appropriately configured to handle such a download is in place, and with the written approval of the DAA.	
Initiative Implementation	Download of Mobile Code from a different enclave is not allowed.	
7.F.1	Encryption and E-Mail - E-mail shall conform to the electronic communications and transmission requirements regarding confidentiality stated elsewhere in this manual. In particular, an e-mail message (and associated attachments) shall be appropriately encrypted if during its transmission it may be accessible to individuals who lack either clearance or formal access approval for the information contained in the e-mail (and associated attachments).	
Initiative Implementation	Refer to JEODNET E-Mail Policy in the Enterprise SSP	
7.F.2	Viruses and E-mail – a. The DAA shall ensure that the threat of viruses in e-mail or attachments is addressed. b. Where technically feasible the DAA shall require the use of anti-viral mechanisms to detect and eradicate viruses in incoming and outgoing e-mail and attachments. c. The means employed to address the virus threat shall be stated in the SSP.	

DCID Para	Stated Requirement	C&A Evaluation
	d. The use of anti-viral procedures and mechanisms to detect and eradicate viruses transported by e-mail or attachments does not relieve the ISSO of ensuring that there are procedures and mechanisms (e.g., central choke points where diskettes are scanned for viruses prior to distribution within the IS) in place to safeguard against virus infection of the IS from other sources.	
Initiative Implementation	Norton Antivirus Corporate software is activated on all servers to include Exchange servers	
7.G.3.a	Collaborative Computing Protection Levels - Collaborative computing mechanisms shall be hosted only on systems operating at Protection Levels 1, 2, and 3, and between systems that process information of the same classifications. But hosting collaborative computing mechanisms on systems operating at Protection Level 3 requires the explicit, written approval of the DAA, and the DAA may impose additional technical or other security safeguards as needed.	
Initiative Implementation		
7.G.3.b	Collaborative Computing Remote Activation - Collaborative computing mechanisms shall not be remotely activated. Activation requires an explicit action by the workstation user (e.g., in the case of a desktop video teleconference, the user of the desktop shall be required to take an explicit action to turn on the camera and microphone, remote users shall not be allowed to activate a user's camera or microphone remotely).	
Initiative Implementation	No collaborative computing services are provided.	
7.G.3.c	Peer-to-Peer Collaborative Computing - Peer-to-peer collaborative computing mechanisms between systems operating at Protection Level 2 shall be configured to ensure that only the information on the screen is observable to the remote user. Information located elsewhere on the workstation shall not be observable, nor shall the remote user be able to modify or delete any information on the workstation. These restrictions also apply to any other IS to which the user's workstation is logically connected (e.g., any logically mounted disks).	
Initiative Implementation		
7.G.3.d	Collaborative Computing Audio/Video Indication - Collaborative computing mechanisms that provide video and/or audio conference capabilities shall provide some explicit indication that the video and audio mechanisms are operating. *IC If a collaborative computing system uses a camera or microphone, then the ambient environment may not exceed the classification level of the collaborative system.*	
Initiative Implementation		
7.G.3.e	DAA Approval for Collaborative Computing - Running collaborative computing mechanisms on mission-critical systems is discouraged and shall require explicit, written DAA approval.	
Initiative Implementation		
7.G.3.f	Collaborative Computing Server Authentication - The server portion of the client-server collaborative computing mechanism shall authenticate all users or processes acting on their behalf.	
Initiative Implementation		
7.G.3.g	Collaborative Computing Session Warnings - While conducting a collaborative	

DCID Para	Stated Requirement	C&A Evaluation
	computing session, the user shall take all reasonable measures to ensure that no sensitive information is inadvertently made either audibly or visually accessible to the collaborative computing mechanism. This includes advising all personnel in the immediate area that the collaborative computing mechanism will be operating.	
Initiative Implementation		
7.G.3.h	Collaborative Computing Session Disconnection - Once the collaborative session is completed, the user shall immediately take an explicit action to disconnect/terminate the collaborative computing mechanism.	
Initiative Implementation		
7.G.3.I	Coll Computing Unattended Ops - Users shall not leave the workstation unattended while a peer-to-peer collaborative computing mechanism is in progress.	
Initiative Implementation		
8.B.1.b	Process and Documentation Training - All individuals involved in the Certification and Accreditation (C&A) process shall be trained in that process and in its documentation requirements.	
Initiative Implementation	Met by restricting involvement to individuals with prior C&A experience.	
8.B.1.b.1	Minimum C&A Training Requirements - As a minimum, [C&A process] training shall include the following: a. System security regulations and policies (individuals shall have the ability to implement and interpret national and agency/department regulations and policies). b. Common information security technologies and practices. c. Testing and evaluation techniques. d. Risk management concepts. e. Interconnected systems security concepts. f. Procedures for incident handling. g. C&A concepts, policies, and procedures. h. Audit analysis procedures and tools.	
Initiative Implementation	JEODNET CA Training meets these requirements refer to the training plan	
8.B.1.b.3	ISSM Training Requirements - In addition to the requirements specified in [DCID 6/3, 8.1.B.1.b.1], ISSMs shall have training in the destruction and release procedures for systems, components, and media.	
Initiative Implementation	CA training covers this material refer to the training plan	
8.B.1.b.4	ISSO Training Requirements - In addition to the requirements specified in [DCID 6/3, 8.1.B.1.b.1], ISSOs shall have the following training: a. How to implement common information systems security practices and technologies. This training shall include information on support infrastructures, help teams, and organizations that could assist the ISSO. b. How to implement testing and evaluation procedures. c. How to implement configuration management concepts. d. Destruction and release procedures for systems, components, and media. e. Other security disciplines that affect the ISSO's operations.	
Initiative Implementation	ISSO training meets these requirements refer to the training plan	
8.B.1.c.1	Training Requirements for Privileged Users - Privileged Users [shall be trained in	

DCID Para	Stated Requirement	C&A Evaluation
	their responsibilities and those of their subordinates], with training to include: a. How to protect the physical area, media, and equipment (e.g., locking doors, care of diskettes). b. How to protect authenticators and operate the applicable system security features. c. Security consequences and costs so that security can be factored into their decisions (manager). d. How to implement and use specific access control products (system administrators). e. How to recognize and report potential security vulnerabilities, threats, security violations, or incidents. f. The organization's policy for protecting information and systems and the roles and responsibilities of various organizational units with which they may have to interact. g. The system security regulations and policies. h. What constitutes misuse or abuse of system privileges.	
Initiative Implementation	training meets these requirements refer to the training plan	
8.B.1.c.2	Training Requirements for General Users - General Users [shall be trained in their responsibilities and those of their subordinates], with training to include: a. How to protect the physical area, media, and equipment (e.g., locking doors, care of diskettes). b. How to protect authenticators and operate the applicable system security features. c. How to recognize and report security violations and incidents. d. The organization's policy for protecting information and systems.	
Initiative Implementation	training meets these requirements refer to the tra ining plan	
8.B.2.a.1	Marking of Removable Media - Removable information storage media shall bear external labels indicating the security classification of the information and applicable associated security markings, such as handling caveats and dissemination control labels. SSPs shall identify the removable storage media to be used with a system. Classified removable media shall be controlled and protected in a manner similar to that used for classified paper materials. Removable media shall be marked as classified if the media has ever been used on the classified system, AND during any use on the system, was writeable (i.e., the write-protect feature could not be verified).	
Initiative Implementation	Use of removable media is eliminated where practicable. Removable media is labeled with the appropriate classification markings.	
8.B.2.a.1.a	Handling of Unmarked Media - In those areas, designated in the SSP, where classified information is processed, unmarked media that are not in factory-sealed packages shall be protected at the highest level of classification processed within the facility, until the media has been reviewed and appropriately labeled.	
Initiative Implementation	All media that is not in a factory-sealed package should bear appropriate markings. If the markings are missing, the media will be handled at the facility high-water-mark.	
8.B.2.a.1.b	Handling of Unclassified Media - In those areas, designated in the SSP, where both classified and unclassified information are processed or stored, unclassified media labels (SF 710) shall be used to identify media that contain only unclassified information.	

DCID Para	Stated Requirement	C&A Evaluation
Initiative Implementation	Unclassified media must be marked with the appropriate SF 710 media label.	
8.B.2.a.2	Marking of Non-removable Media - Non-removable information storage media shall bear external labels indicating the security classification of the information and applicable associated security markings, such as handling caveats and dissemination control labels. If it is difficult to mark the non-removable media itself, the labels described below may be placed in a readily visible position on the cabinet enclosing the media.	
Initiative Implementation	Non-removable media or the containing cabinet will bear the appropriate external labels.	
8.B.2.a.3.a	External Labels [Protection Levels 1,2,3] - For a system operating at Protection Level 1, 2, or 3, storage media shall bear external labels indicating the highest classification level and applicable associated security markings of information ever processed on the system, unless a reliable human review of the media's entire contents is performed.	
Initiative Implementation	Storage media will bear external labels indicating the system's highest classification level unless a reliable human review is performed of the media'a entire contents.	
8.B.2.a.3.b	External Labels [Protection Levels 4,5] - For a system operating at Protection Level 4 or 5, storage media shall be labeled with the classification level and applicable associated security markings of information on the media.	
Initiative Implementation	N/A	
8.B.2.b	Marking Hardware Components - Procedures identified in the SSP shall be implemented to ensure that all components of an IS, including input/output devices that have the potential for retaining information,* terminals, standalone microprocessors, and word processors used as terminals, bear a conspicuous, external label stating the highest classification level and most restrictive classification category of the information accessible to the component in the IS. This labeling may consist of permanent markings on the component or a sign placed on the terminal. [*For example, mice and trackballs do not normally retain information.]	
Initiative Implementation	All components of the system will be marked appropriately.	
8.B.2.c	Marking Human-Readable Output - Human-readable output shall be marked appropriately, on each human-readable page, screen, or equivalent (e.g., the proper classification must appear on each classified microfiche and on each page of text on the fiche).	
Initiative Implementation		
8.B.2.c.1	Banner Page - Except as provided by the DAA, the first page of the output (the banner page) shall include a warning message reminding the person receiving the output to control every page according to the markings on the banner page until a reliable human review has determined that the output is marked appropriately.	
Initiative Implementation		
8.B.2.c.1.a	Manual Banner Page - If the capability to provide automatic banner pages does not exist, procedures shall be developed to mark manually or otherwise assure review of printed output, as appropriate. *IC If the capability to provide automatic banner pages does not exist, procedures	

DCID Para	Stated Requirement	C&A Evaluation
	shall be developed to mark individual pages manually (e.g., to mark with a rubber stamp).*	
Initiative Implementation		
8.B.2.c.1.b	Distribution of Output - Using procedures approved by the Data Owner or responsible official, explicit approval shall be obtained from the DAA or his designee before forwarding output, which has not had a reliable human review for appropriate security classification and marking, to recipients who do not have system access. Such approval(s) can be for a specific release, for the overall release procedure(s), or for both.	
Initiative Implementation		
8.B.2.c.2	Marking Printed Output - Individual pages of output shall be marked as appropriate either (a) to reflect the classification and applicable associated security markings of the data that is printed on each page, or (b) with the highest classification and all applicable associated security markings of the data that is to be printed.	
Initiative Implementation		
8.B.2.c.3.a	Marking Output From Shared Printers (PL 1, 2, 3) - At the DAA's discretion, systems operating at Protection Level 1, 2, or 3 shall mark the beginning (banner) page of all human-readable, paged, hardcopy output (printer output) with a human-readable representation of the system's security parameter, which is the highest classification and all appropriate associated security markings of the information processed by the system. For Protection Level 3, procedures shall be implemented to ensure output is given only to authorized users.	
Initiative Implementation		
8.B.2.d	Marking Variations - DAAs or their designees may identify specific types of media or hardware components that need not be marked in accordance with this policy so long as they remain within a single, secure environment, and: 1. All systems are operating at the same classification level and access authorizations; 2. The media or hardware components are documented in the SSP 3. Mechanisms or procedures have been established to provide the security protection intended by this policy; 4. If removed from the single, secure environment, the media are either appropriately marked or sanitized or declassified in accordance with paragraph 8.B.5, below.	
Initiative Implementation	N/A	
8.B.2.e	Marking of Removable System Media - Removable system media shall be externally marked with the established classification label (or a facsimile of it), specified in [DCID 6/3] Table 8-1 and published by the Information Security Oversight Office (ISOO).	
Initiative Implementation	All removable media will be marked appropriately.	
8.B.2.g	Location of Security Labels - Security labels shall be conspicuously placed on media; however, their placement must not adversely affect the operation of the equipment on which the media is used. A security label may be placed on the protective cover rather than on the media only if labeling the media would impair	

DCID Para	Stated Requirement	C&A Evaluation
	operation or if the media is too small to accommodate a label. The intent of marking is to provide a visible indicator of content to support proper handling and storage of the media. *IC When the classification of the media increases to a higher level, replace the classification label with the appropriate higher classification-level label.*	
Initiative Implementation	All equipment markings will be conspicuously placed.	
8.B.2.i	Downgrading or Declassification - The downgrading or declassification instructions applicable to the data contained on the portable system media shall accompany the data when it is transferred from one security control point to another. These instructions may be internal to the media.	
Initiative Implementation	Refer to the JEODNET downgrade and declassification policy	
8.B.3	Manual Review of Human-Readable Output. - Before human-readable output is released outside the security boundary, an appropriately authorized individual shall provide a reliable human review of the output to determine whether it is accurately marked with the appropriate classification and applicable associated security markings. The authorized reviewer shall be knowledgeable enough about the data to determine the presence of improper data in the information being reviewed, and shall be cleared for and have formal access approval for he information being reviewed. The review shall be at a level of detail, as set forth by the DAA, to allow the reviewer to accept security responsibility for releasing the data to its recipient.	
Initiative Implementation	Reliable human review will be performed to verify proper markings.	
8.B.3.a	Manual Review of Softcopy - The electronic output (i.e., softcopy) to be released outside the security boundary shall be verified by a review (in human-readable form) of all data including embedded text (e.g., headers and footers, hidden text, notes, edited text, control characters) before being released.	
Initiative Implementation	Reliable human review will be performed to verify proper markings.	
8.B.3.b	Examination of Electronic Media - Information on media that is not in human-readable form (e.g., embedded graphics, sound, video, imagery) shall be examined for content with the appropriate software, hardware, and firmware. Care is required to ensure that all layers or levels of the graphics or image are reviewed.	
Initiative Implementation		
8.B.5.b.1	Reuse of media - Cleared or sanitized media that has previously contained classified information may be reused at the same classification level (e.g., TS -> TS), or at a higher level (e.g., S ->TS). Sanitized media may be downgraded or declassified with the DAA's and, as applicable, the Data Owner's approval as specified in the SSP. Only approved equipment and software shall be used to overwrite and degauss magnetic media containing classified information. Each action or procedure taken to overwrite or degauss such media shall be verified.	
Initiative Implementation	Refer to Enterprise SSP to reuse media appropriately.	
8.B.5.b.2	Clearing - Only approved equipment and overwriting software that is compatible with the specific hardware for overwriting shall be used to clear media that have contained classified information. Use of such software shall be coordinated in advance with the DAA. The success of the overwrite procedure shall be verified through random sampling of the overwritten media. Items that have been cleared (i.e., not sanitized) shall remain at the previous level of classification and remain in	

DCID Para	Stated Requirement	C&A Evaluation
	a secure, controlled environment.	
Initiative Implementation	Refer to Enterprise SSP to use approved overwriting software for clearing media.	
8.B.5.b.3.a	Sanitizing Media Containing Classified Info - Magnetic media containing classified information can be sanitized by use of an approved degaussing procedure. The DAA, with the Data Owner's approval (if applicable), can allow overwriting of some types of classified information as a sanitizing procedure.	
Initiative Implementation	Refer to Enterprise SSP to use approved degaussing methods for sanitization of media.	
8.B.5.b.4	Optical Disks - Optical disks (including compact disk/read only memory, write once/read many, Digital Versatile Disk, and writeable compact discs) offer no mechanism for sanitization and must be destroyed via incineration or any other NSA-approved method. They should be placed in a classified trash bag labeled "non-soluble" and disposed as classified waste.	
Initiative Implementation	Optical disks are not being used.	
8.B.5.c	Malfunctioning Media - Magnetic storage media that malfunctions or contains features that inhibit overwriting or degaussing shall be reported to the ISSO, who will coordinate repair or destruction with the responsible DAA.	
Initiative Implementation	Site SOP	
8.B.5.d.2	Volatile Memory Components - Memory components that do not retain data after removal of all electrical power sources, and when re-inserted into a similarly configured system do not contain residual data, are considered volatile memory components. Volatile components that have contained classified information may be released only in accordance with procedures developed by the ISSO and stated in the SSP. A record shall be maintained of the equipment release indicating that, per a best engineering assessment, all component memory is volatile and that no data remains in or on the component when power is removed.	
Initiative Implementation	All component memory used in JEODNET servers is volatile.	
8.B.5.d.3	Nonvolatile Memory Components - Components that do retain data when all power sources are discontinued are nonvolatile memory components; these include read-only memory (ROM), programmable ROM (PROM), or erasable PROM (EPROM), and their variants. Those that have been programmed at the vendor's commercial manufacturing facility, and are considered to be unalterable in the field, may be released. All other nonvolatile components may be released after successful completion of the procedures outlined in NSA/CSSM 130-2. Failure to accomplish these procedures shall require the ISSO to coordinate with the DAA for a determination of releaseability.	
Initiative Implementation	Appropriate procedures will be followed.	
8.B.5.e	Release of Systems and Components - The ISSO shall develop equipment removal procedures for systems and components that have processed or contained classified or extremely sensitive information; these procedures shall be stated in the SSP. When such equipment is no longer needed, it can be released after: Inspection of the system equipment by the ISSO or designee. This review shall assure that all media, including internal disks, have been removed or sanitized. [Creating a] record of the equipment release indicating the procedure used for sanitization, and to whom the equipment was released. This record shall be retained for a period prescribed by the DAA.	

DCID Para	Stated Requirement	C&A Evaluation
Initiative Implementation	Media will be removed or sanitized before equipment release..	
8.B.6.a	DAA Approval for Equipment Co-location - DAA approval is necessary to co-locate classified and unclassified ISs in a Sensitive Compartmented Information Facility (SCIF). *IC References to "unclassified" systems should be interpreted as "lower classified" systems which includes all levels less than that of the subject system (including unclassified).*	
Initiative Implementation	Site dependent whether co-location is required.	
8.B.6.b.1	Co-location Marking - An IS approved for processing unclassified information must be clearly marked as such when located within a SCIF.	
Initiative Implementation	All systems will be marked appropriately for the level of data processed.	
8.B.6.b.2	Co-location Separation - An IS approved for processing unclassified information must be physically separated from any classified IS.	
Initiative Implementation	No physical connection made between classified and unclassified systems unless a SABI or DIAP approved cross domain solution is used.	
8.B.6.b.3	Co-location Connection - An IS approved for processing unclassified information must not be connected to any classified IS without the PAA's written approval.	
Initiative Implementation	No physical connection made between classified and unclassified systems unless a SABI or DIAP approved cross domain solution is used.	
8.B.6.b.4	Co-location Training - Users must be provided with co-location process and procedures as part of their required security and awareness training.	
Initiative Implementation	Site dependent	
8.B.6.b.5	Co-location Documentation - The ISSO must document in the SSP the procedures and technical safeguards to ensure the protection of classified information.	
Initiative Implementation		
8.B.6.b.6	Co-location Media Handling - All unmarked media must be treated as classified at the highest level processed by the facility until reviewed and verified.	
Initiative Implementation	Refer to policy set forth in the Enterprise SSP	
8.B.6.c	Co-located Portable Equipment - An unclassified portable IS (including personally owned ISs) is prohibited in a SCIF unless the DAA specifically permits its use. If permitted, all personnel shall adhere to the following procedures: 1. Connection of an unclassified portable IS to a classified IS is prohibited. 2. Connection of an unclassified IS to another unclassified IS may be done only with the DAA's written approval. 3. Use of an internal or external modem with the IS device is prohibited within the SCIF without the DAA's written approval. 4. The portable ISs and the contained data are subject to random reviews and inspections by the ISSO/ISSM. If classified information is found on the portable IS it shall be handled in accordance with the incident handling policy.	
Initiative Implementation	Unclassified portable equipment usage will be appropriately restricted.	
8.B.7.a	Incident Reporting Program - A formal incident-reporting program shall be put in place, and it shall be evaluated on a regular basis by the DAA. All security incidents shall be reported to the DAA and the Data Owner through the incident-	

DCID Para	Stated Requirement	C&A Evaluation
	reporting system. All incidents that may affect (or have affected) systems under more than one DAA shall be reported to the DAA responsible for the affected system. As appropriate, the information shall be forwarded to other involved DAAs and Data Owners. Additionally, organizational investigative agencies shall be immediately apprised of all security incidents and, if deemed necessary and appropriate, shall participate in their resolution.	
Initiative Implementation	Refer to policy set forth in the Enterprise SSP	
8.B.7.b	Incident Reporting Procedures - Procedures shall be developed by the ISSM and approved by the DAA to provide the appropriate responses to incidents.	
Initiative Implementation	Refer to JEODNET Enterprise Contingency Policy	
8.B.8.a.1	Maintenance Personnel Clearance - Except as authorized by the DAA, personnel who perform maintenance on systems shall be cleared to the highest classification level of information on the system, and indoctrinated for all information processed on that system. Cleared personnel who perform maintenance or diagnostics on an IS do not require an escort, unless need-to-know controls must be enforced. However, an appropriately cleared and, when possible, technically knowledgeable, facility employee shall be present within the area where the maintenance is being performed to assure that the proper security and safety procedures are being followed.	
Initiative Implementation	No onsite maintenance by improperly cleared personnel. Cleared personnel without need-to-know access will be escorted.	
8.B.8.a.2	Cleared Foreign National Maint Personnel - Cleared foreign nationals may be utilized as maintenance personnel for those systems jointly owned and operated by the US and a foreign allied government, or those owned and operated by foreign allied governments. Approvals, consents, and detailed operational conditions must be fully documented within a Memorandum of Agreement. *IC Section 8.B.8.a.2 is not applicable to industry.*	
Initiative Implementation	No onsite maintenance by improperly cleared personnel.	
8.B.8.b.1	Uncleared (or Lower Cleared) Maintenance Personnel - If appropriately cleared personnel are unavailable to perform maintenance, an uncleared person, or one cleared to a lower level, may be used provided a fully cleared and technically qualified escort monitors and records that person's activities in a maintenance log.	
Initiative Implementation	No onsite maintenance by improperly cleared personnel.	
8.B.8.b.2	Citizenship of Maintenance Personnel - For US-owned and operated ISs, uncleared/lower-cleared maintenance personnel must be US citizens. For systems jointly owned and operated by the US and a foreign allied government, or those owned and operated by foreign allied governments, uncleared/lower-cleared foreign nationals may be used. Approvals, consents, and detailed operational conditions must be fully documented within a Memorandum of Agreement. *IC Section 8.B.8.b.2 is not applicable to industry.*	
Initiative Implementation	No onsite maintenance by improperly cleared personnel.	
8.B.8.b.3	Prep for Uncleared/Lower Cleared Maintenance - Prior to maintenance by uncleared/lower-cleared personnel, the IS shall be completely cleared and all nonvolatile data storage media removed or physically disconnected and secured. When a system cannot be cleared, DAA-approved procedures shall be enforced to deny the uncleared/lower-cleared individual visual and electronic access to any	

DCID Para	Stated Requirement	C&A Evaluation
	classified or sensitive data that is contained on the system.	
Initiative Implementation	No onsite maintenance by improperly cleared personnel.	
8.B.8.b.4	OS Maintenance Copy - A separate, unclassified copy of the operating system and application software, including any micro-coded floppy disks, cassettes, or optical disks that are integral to the IS, shall be used for all maintenance operations performed by uncleared/lower-cleared personnel. The copy shall be labeled "UNCLASSIFIED-FOR MAINTENANCE ONLY" and protected in accordance with procedures established in the SSP. The ISSM must consider on a case-by-case basis maintenance procedures for an information system whose operating system resides on a non-removable storage device.	
Initiative Implementation	No onsite maintenance by improperly cleared personnel.	
8.B.8.c.1	Maintenance Logs - A maintenance log shall be maintained. The maintenance log shall include the date and time of maintenance, name of the individual performing the maintenance, name of escort, and a description of the type of maintenance performed, to include identification of replacement parts.	
Initiative Implementation	Each server has a combined installation/maintenance log documenting what has been modified and by whom. This is also a function of the Enterprise Management System	
8.B.8.c.3	Removal of Equipment for Maintenance - If systems or system components are to be removed from the facility for repair, they shall first be purged, and downgraded to an appropriate level, or sanitized of all classified data and declassified in accordance with DAA-approved procedures. The ISSO or designee shall approve the release of all systems and all parts removed from the system (see section on Release of Memory Components and Boards).	
Initiative Implementation	Equipment removed will be downgraded appropriately.	
8.B.8.c.4	Use of Network Analyzers - Introduction of network analyzers (e.g., sniffers) that would allow the maintenance personnel the capability to do promiscuous mode (real time) monitoring shall be approved by the ISSM or designee prior to being introduced into an IS.	
Initiative Implementation	Site dependent. Function provided by the Enterprise Management and Intrusion Detection System	
8.B.8.c.5	Diagnostic Test Programs - If maintenance personnel bring diagnostic test programs (e.g., software/firmware used for maintenance or diagnostics) into a facility, the media containing the programs (1) shall be checked for malicious code before the media is connected to the system, (2) shall remain within the facility, and (3) shall be stored and controlled at the level of the IS. Prior to entering the facility, the maintenance personnel shall be advised that they will not be allowed to remove media from the facility. If deviation from this procedure is required under special circumstances, then each time the diagnostic test media is introduced into a facility, the media shall undergo stringent integrity checks (e.g., virus scanning, checksum) prior to being used on the IS and, before leaving the facility, the media shall be checked to assure that no classified information has been written on it. Such a deviation requires approval by the ISSM.	
Initiative Implementation	Site dependent.	
8.B.8.c.6	Diagnostic Equipment - All diagnostic equipment and other devices carried into a facility by maintenance personnel shall be handled as follows:	

DCID Para	Stated Requirement	C&A Evaluation
	a. Systems and system components being brought into the facility shall be inspected for obvious improper modification. b. Maintenance equipment that has the capability of retaining information shall be appropriately sanitized by procedures outlined in paragraph 8.B.5 before being released. If the equipment cannot be sanitized, the equipment shall remain within the facility, be destroyed, or be released under procedures approved by the DAA and the Data Owner(s) or responsible official(s). c. Replacement components that are brought into the facility for the purpose of swapping with facility components are allowed. However, any component placed into an IS shall remain in the facility until proper release procedures are completed. Any component that is not placed in an IS may be released from the facility. d. Communication devices with transmit capability (e.g., pagers, [RF] LAN connections) belonging to the maintenance personnel or any data storage media not required for the maintenance visit shall remain outside the system facility for return to the maintenance personnel upon departure from the facility.	
Initiative Implementation	Site dependent.	
8.B.8.c.7	Security Maintenance Changes - Maintenance changes that impact the security of the system shall receive a configuration management review.	
Initiative Implementation	Must pass both the JEODNET CCB	
8.B.8.c.8	Post-maintenance Security Review - After maintenance has been performed, the security features on the IS shall be checked to assure that the IS is still functioning properly.	
Initiative Implementation	Appropriate sections of the certification testing will be re-run.	
8.B.8.d.1	Performance of Remote Maintenance or Diagnostics - Remote diagnostic or maintenance services are acceptable if performed by a service or organization that provides the same level and category(ies) of security as the IS. The communications links connecting the components of the systems, associated data communications, and networks shall be protected in accordance with national policies and procedures applicable to the sensitivity level of the data that may be transmitted over the link.	
Initiative Implementation	No remote maintenance accept as part of the Enterprise Management System.	
8.B.8.d.2	Remote Maintenance Security Requirements - If remote diagnostic or maintenance services are required from a service or organization that does not provide the same level of security required for the system being maintained, the IS shall be sanitized and physically separated from other information systems prior to the connection of the remote access line. If the system cannot be sanitized (e.g., due to a system failure), remote maintenance shall not be allowed.	
Initiative Implementation	No remote maintenance accept as part of the Enterprise Management System.	
8.B.8.d.3	Remote Maintenance Additional Requirements - Initiation and termination of the remote access shall be performed by the ISSO or designee. Keystroke monitoring shall be performed on all remote diagnostic or maintenance services. A technically qualified person shall review the maintenance log, and if appropriate, the audit log to assure the detection of unauthorized changes. The ISSM/ISSO shall assure that maintenance technicians responsible for performing remote diagnosis/maintenance are advised (e.g., contractually, verbally, or by banner) prior to remote diagnostics/maintenance activities that keystroke monitoring will be performed. Unless an exception has been granted by the DAA, maintenance personnel	

DCID Para	Stated Requirement	C&A Evaluation
	accessing the information systems at the remote site shall be cleared to the highest level of information processed on that system, even if the system was downgraded/sanitized prior to remote access. Installation and use of remote diagnostic links shall be specifically addressed in the SSP and agreed to by the DAA. An audit log shall be maintained of all remote maintenance, diagnostic, and service transactions including all commands performed and all responses. The log shall be periodically reviewed by the ISSO.	
Initiative Implementation	No remote maintenance accept as part of the Enterprise Management System.	
8.B.8.d.5	Remote Maintenance Passwords - Passwords used during the maintenance process shall be changed following each remote diagnostic maintenance service. All passwords are assigned and controlled by the information system's ISSM or ISSO.	
Initiative Implementation	No remote maintenance accept as part of the Enterprise Management System.	
8.C.1	Communications Security - The communications links connecting the components of the systems, associated data communications, and networks shall be protected in accordance with national policies and procedures applicable to the sensitivity level of the data being transmitted.	
Initiative Implementation	Site dependent.	
8.C.2.b	Uncleared Developers - Uncleared personnel developing hardware, firmware, software, or data files shall not, to the maximum extent possible, have any knowledge that the software, hardware, firmware or data files will be used in a classified area. Before hardware, firmware, software, or data files that are developed or modified by uncleared personnel can be used in a classified processing period, appropriately cleared, technically knowledgeable personnel shall review them to ensure that no security vulnerabilities or malicious code exist. Software, hardware, and firmware used for maintenance or diagnostics shall be maintained within the secure computing facility and, even though unclassified, shall be separately controlled.	
Initiative Implementation	All JEODNET development personnel cleared for Secret NOFORN.	
8.C.2.c	Security-related Hardware, Software, and Firmware - Personnel responsible for installing modifications to system- or security-related software, hardware, and firmware or data files on a classified IS shall be cleared to the highest level of information processed or stored. Software, hardware, and firmware that contains security-relevant functions (e.g., sanitization, access control, auditing) shall be validated by the ISSO to confirm that security-related features are fully functional, protected from modification, and effective.	
Initiative Implementation	All JEODNET personnel cleared for Secret NOFORN.	
8.C.3	EMSEC/TEMPEST - The components of the systems, associated data communications, and networks shall be protected in accordance with national EMSEC/TEMPEST policies and procedures applicable to the sensitivity level of the data being transmitted.	
Initiative Implementation	Site dependent	
8.C.4	Technical Surveillance Countermeasures (TSCM) - The components of the systems, associated data communications, and networks shall be protected in accordance with national TSCM policies and procedures applicable to the sensitivity level of the data being transmitted.	

DCID Para	Stated Requirement	C&A Evaluation
Initiative Implementation	Site dependent	
8.F.1	Foreign Nationals Access Approval - US Government intelligence information is not releasable to foreign nationals except as authorized by the US Government. Data Owners can designate their information as releasable to individuals of specific nationalities in accordance with DCIDs 1/7 and 5/6. PAAs/DAAs shall obtain the written permission of all applicable Data Owners before allowing access by foreign nationals to a system that contains information not releasable to individuals of those nationalities. The decision to allow access by foreign nationals to systems that process intelligence information shall be explicit and shall be in writing.	
Initiative Implementation	No foreign nationals currently granted access to SIPRNET/NIPRNET.	
8.F.2	Foreign Nationals Access of NOFORN - In the absence of reliable human review, a foreign national may access or receive output from a system processing intelligence marked NOFORN only when (a) the system can reliably ensure that all NOFORN data is protected from foreign access, (b) the accrediting authority has obtained written approval from the head of CIA, DIA, NRO, or NSA (as appropriate to the sponsorship of the system in question), and (c) the accrediting authority has obtained concurrence from all Data Owners of NOFORN data processed by the system before any data is accessible, directly or indirectly, by foreign nationals. Failing agreement by the Data Owners to allow the foreign national access, the accrediting authority can appeal to the DCI/DDCI.	
Initiative Implementation	No foreign nationals currently granted access to SIPRNET/NIPRNET.	
9.D.2.b.2	Joint Accreditations of Intelligence Systems - For systems processing intelligence information, operating under the purview of more than one PAA, and that are not jointly certified by a panel or board: a. A Memorandum of Agreement (MOA) shall be required between the cognizant PAAs; the MOA should name a lead PAA, who will be responsible for the system certification. If no lead PAA is named, then both parties shall share responsibility. b. The MOA shall be included in the SSP.	
Initiative Implementation	N/A	
9.D.3.b.2	Site-Based Accreditation - A Site Security CONOPS and a Site Security Architecture are required for site-based accreditation and shall contain a listing of all systems covered under the site-based accreditation, a description of how the site complies with the requirements of this manual, and a wiring diagram showing external connections.	
Initiative Implementation	Contained in System Security Plan.	
9.D.3.c.4	Interconnected Systems - A interconnection Security Agreement (ISA) is required whenever an accredited system is connected to a system accredited by a different DAA.* The contents of such an ISA are specified in Appendix A. [*Some types of interconnected networks, particularly those that are community wide, do not require a formal ISA. In this case, the function of the ISA is handled with a list of requirements to be satisfied prior to connection. Upon verification that the list has been satisfied, the interconnection is made.]	
Initiative Implementation	N/A	
9.G.4	Tactical or Deployable Systems - A tactical system may be part of a fixed location or maintained in a deployable configuration so that it can be moved quickly to another location to support operational mission requirements. The system can	

DCID Para	Stated Requirement	C&A Evaluation
	operate in a stand-alone mode or be attached via communications to a mobile or fixed facility under an extended LAN or WAN configuration. Tactical systems shall provide the appropriate Protection Level and Levels-of-Concern based upon the operating environment, network connection requirements, portability, and degree of access to other systems. The Protection Level and Levels-of-Concern shall be applied while the system is in-garrison, in-transit, and/or deployed. The DAA may require additional security requirements or safeguards for tactical systems while in-transit or in the deployed environment.	
Initiative Implementation		
9.G.5.b	ISs With Group Authenticators - In general, the use of group authenticators precludes the association of a particular act with the individual who initiated that act. In turn, this can preclude assignment of responsibility and can exacerbate the difficulties involved in incident investigation. DAAs shall avoid situations in which the group authenticator is effectively the sole access control mechanism for the system. Use of group authenticators for broader access after the use of a unique authenticator for initial identification and authentication carries much less risk. The use of group authenticators shall be explicitly authorized by the DAA..	
Initiative Implementation	Group authenticators are not employed by JEODNET.	
9.G.5.c	ISs With Group Authenticators - Positions and applications requiring the use of group authenticators shall be discussed in the SSP.	
Initiative Implementation	Group authenticators are not employed by JEODNET.	
9.G.6.b	Information Systems Using Periods Processing - As long as the sanitization procedures between each Protection Level segment have been approved by the DAA based on guidelines from the Data Owner(s) or responsible official(s), the IS need meet only the security requirements of each processing period, while in that period. If the sanitization procedures for use between periods are approved by the DAA(s), the security requirements for a given period are considered in isolation, without consideration of other processing periods. Such sanitization procedures shall be detailed in the SSP.	
Initiative Implementation	Periods processing does not apply to JEODNET	